

Prestige 652

ADSL Security Router

User's Guide

Version 3.40

August 2002

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2002 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Refer to the product page at www.zyxel.com.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada label does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, Taiwan 300, R.O.C.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH, Adenauerstr. 20/A4 D-52146 Wuerselen, Germany
MALAYSIA	support@zyxel.com.my sales@zyxel.com.my	+603-795-44-688 +603-795-34-407	www.zyxel.com.my	Lot B2-06, PJ Industrial Park, Section 13, Jalan Kemajuan, 46200 Petaling Jaya Selangor Darul Ehasn, Malaysia

Table of Contents

GETTING STARTED	I
Chapter 1 Getting To Know Your Prestige.....	1-1
1.1 Prestige 652 ADSL Security Router	1-1
1.2 Features	1-1
1.3 Applications for the Prestige 652	1-6
Chapter 2 Hardware Installation and Initial Setup	2-1
2.1 Front Panel LEDs of the P652.....	2-1
2.2 Rear Panel and Connections.....	2-2
2.3 Additional Installation Requirements.....	2-3
2.4 P652 with POTS.....	2-4
2.5 P652 with ISDN	2-6
2.6 Turning On Your Prestige	2-7
2.7 Configuring Your Prestige For Internet Access	2-7
2.8 Resetting the Prestige	2-8
2.9 Navigating the SMT Interface.....	2-10
2.10 Changing the System Password	2-13
Chapter 3 General Setup	3-1
3.1 System Name	3-1
3.2 Dynamic DNS	3-1
3.3 General Setup	3-2
3.4 LAN Setup	3-4
3.5 Protocol Dependent Ethernet Setup	3-5
Chapter 4 Internet Access	4-1
4.1 Factory Ethernet Defaults.....	4-1
4.2 LANs and WANs	4-1
4.3 TCP/IP Parameters	4-2
4.4 IP Multicast	4-5
4.5 IP Policies	4-5
4.6 IP Alias.....	4-5
4.7 Route IP Setup.....	4-8
4.8 TCP/IP Ethernet Setup and DHCP.....	4-8
4.9 VPI and VCI.....	4-11
4.10 Multiplexing.....	4-11
4.11 Encapsulation	4-11
4.12 IP Address Assignment	4-12
4.13 Internet Access Configuration.....	4-13
Advanced Applications	II

Chapter 5 Remote Node Configuration	5-1
5.1 Remote Node Setup	5-1
5.2 Remote Node Setup	5-6
5.3 Remote Node Filter	5-8
Chapter 6 Remote Node TCP/IP Configuration.....	6-1
6.1 TCP/IP Configuration	6-1
Chapter 7 Bridging Setup	7-1
7.1 Bridging in General.....	7-1
7.2 Bridge Ethernet Setup	7-1
Chapter 8 Network Address Translation (NAT).....	8-1
8.1 Introduction.....	8-1
8.2 Using NAT.....	8-6
8.3 NAT Setup	8-8
8.4 NAT Server Sets – Port Forwarding	8-16
8.5 General NAT Examples	8-20
FIREWALL AND CONTENT FILTERS.....	III
Chapter 9 Firewalls.....	9-1
9.1 What Is a Firewall?	9-1
9.2 Types of Firewalls.....	9-1
9.3 Introduction to ZyXEL’s Firewall	9-2
9.4 Denial of Service	9-3
9.5 Stateful Inspection	9-7
9.6 Guidelines For Enhancing Security With Your Firewall	9-11
9.7 Packet Filtering Vs Firewall	9-12
Chapter 10 Introducing the Prestige Firewall.....	10-1
10.1 Remote Management and the Firewall	10-1
10.2 Access Methods	10-1
10.3 Using Prestige SMT Menus	10-1
Chapter 11 Using the Prestige Web Configurator.....	11-1
11.1 Web Configurator Login and Main Menu Screens	11-1
11.2 Enabling the Firewall.....	11-2
11.3 E-mail	11-2
11.4 Attack Alert.....	11-6
Chapter 12 Creating Custom Rules	12-1
12.1 Rules Overview.....	12-1
12.2 Rule Logic Overview	12-1
12.3 Connection Direction.....	12-3
12.4 Rule Summary	12-4
12.5 Predefined Services.....	12-6
12.6 Timeout.....	12-13
Chapter 13 Customized Services	13-1

13.1	Introduction	13-1
13.2	Creating/Editing A Customized Service	13-3
13.3	Example DHCP Negotiation and Syslog Connection from the Internet	13-4
Chapter 14	Logs	14-1
14.1	Log Screen	14-1
Chapter 15	Content Filtering	15-1
15.1	Keyword	15-1
15.2	Schedule	15-1
15.3	Trusted	15-1
15.4	Logs	15-1
	Advanced Management	IV
Chapter 16	Filter Configuration	16-1
16.1	About Filtering	16-1
16.2	Configuring a Filter Set	16-4
16.3	Configuring a Filter Rule	16-9
16.4	Filter Types and NAT	16-16
16.5	Example Filter	16-16
16.6	Applying Filters and Factory Defaults	16-19
Chapter 17	SNMP Configuration	17-1
17.1	About SNMP	17-1
17.2	Supported MIBs	17-2
17.3	SNMP Configuration	17-2
17.4	SNMP Traps	17-4
Chapter 18	System Information and Diagnosis	18-1
18.1	System Status	18-1
18.2	System Information and Console Port Speed	18-3
18.3	Log and Trace	18-5
18.4	Diagnostic	18-8
18.5	Command Interpreter Mode	18-9
Chapter 19	Firmware and Configuration File Maintenance	19-1
19.1	Filename Conventions	19-1
19.2	Backup Configuration	19-2
19.3	Restore Configuration	19-7
19.4	Uploading Firmware and Configuration Files	19-10
Chapter 20	System Maintenance and Information	20-1
20.1	Command Interpreter Mode	20-1
20.2	Call Control Support	20-2
20.3	Time and Date Setting	20-4
Chapter 21	Remote Management	21-1
21.1	About Telnet Configuration	21-1
21.2	Telnet Under NAT	21-1

21.3	Telnet Capabilities	21-1
21.4	FTP	21-2
21.5	Web	21-2
21.6	Remote Management	21-2
21.7	Remote Management and NAT	21-4
21.8	System Timeout	21-4
Chapter 22	IP Policy Routing	22-1
22.1	Introduction	22-1
22.2	Benefits	22-1
22.3	Routing Policy	22-1
22.4	IP Routing Policy Setup	22-2
22.5	Applying an IP Policy	22-5
22.6	IP Policy Routing Example	22-7
	CALL SCHEDULING, VPN/IPSEC AND INTERNAL SPTGEN	V
Chapter 23	Call Scheduling	23-1
23.1	Introduction	23-1
Chapter 24	Introduction to IPSec	24-1
24.1	Introduction	24-1
24.2	IPSec Architecture	24-3
24.3	Encapsulation	24-5
24.4	IPSec and NAT	24-5
Chapter 25	VPN/IPSec Setup	25-1
25.1	VPN/IPSec Setup	25-1
25.2	IPSec Algorithms	25-2
25.3	IPSec Summary	25-3
25.4	IPSec Setup	25-8
25.5	IKE Setup	25-12
25.6	Manual Setup	25-17
Chapter 26	SA Monitor	26-1
1.1.	Introduction	26-1
Chapter 27	IPSec Log	27-1
27.1	IPSec Logs	27-1
Chapter 28	Internal SPTGEN	28-1
28.1	The Configuration Text File Format	28-1
28.2	Internal SPTGEN FTP Download Example	28-3
28.3	Internal SPTGEN FTP Upload Example	28-4
	ADDITIONAL INFORMATION	VI
Chapter 29	Troubleshooting	29-1
29.1	Problems Starting Up the Prestige	29-1
29.2	Problems with the LAN LED	29-1
29.3	Problems with the DSL LED	29-2

29.4 Problems with the LAN Interface29-2

29.5 Problems with the WAN Interface29-2

29.6 Problems with Internet Access29-3

29.7 Problems with the Password29-3

29.8 Problems with the Web Configurator.....29-4

29.9 Problems with Remote Management29-4

List of Figures

Figure 1-1 Internet Access Application.....	1-7
Figure 1-2 Firewall Application.....	1-8
Figure 1-3 LAN-to-LAN Application.....	1-8
Figure 1-4 VPN Application	1-9
Figure 2-1 Front Panel.....	2-1
Figure 2-2 Rear Panel.....	2-2
Figure 2-3 Connecting a POTS Splitter.....	2-5
Figure 2-4 Connecting a Microfilter.....	2-6
Figure 2-5 P652 with ISDN.....	2-6
Figure 2-6 Power-On Display.....	2-7
Figure 2-7 Login Screen.....	2-8
Figure 2-8 SMT Menu Overview	2-10
Figure 2-9 SMT Main Menu.....	2-12
Figure 2-10 Menu 23 — System Password	2-13
Figure 3-1 Menu 1 — General Setup.....	3-2
Figure 3-2 Configure Dynamic DNS.....	3-3
Figure 3-3 Menu 3 — Ethernet Setup.....	3-5
Figure 3-4 Menu 3.1 — LAN Port Filter Setup.....	3-5
Figure 4-1 LAN & WAN IPs	4-2
Figure 4-2 Physical Network	4-6
Figure 4-3 Partitioned Logical Networks	4-6
Figure 4-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup.....	4-6
Figure 4-5 Menu 3.2.1 — IP Alias Setup.....	4-7
Figure 4-6 Menu 1 — General Setup.....	4-8
Figure 4-7 Menu 3.2 — TCP/IP and DHCP Ethernet Setup	4-9

Figure 4-8 Example of Traffic Shaping.....	4-15
Figure 4-9 Internet Access Setup	4-15
Figure 5-1 Menu 11 — Remote Node Setup.....	5-2
Figure 5-2 Menu 11.1 — Remote Node Profile	5-4
Figure 5-3 Remote Node Network Layer Options	5-7
Figure 5-4 Menu 11.5 — Remote Node Filter	5-9
Figure 5-5 Menu 11.5 — Remote Node Filter (PPPoE or PPPoA Encapsulation)	5-9
Figure 6-1 Menu 11.6 for RFC-1483 or ENET ENCAP with VC-based Multiplexing.....	6-2
Figure 6-2 Menu 11.6 for LLC-based Multiplexing or PPPoA or PPPoE Encapsulation	6-2
Figure 6-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection	6-3
Figure 6-4 Remote Node Network Layer Options	6-5
Figure 6-5 Sample Static Routing Topology	6-7
Figure 6-6 Menu 12 — Static Route Setup	6-8
Figure 6-7 Menu 12.1 — IP Static Route Setup.....	6-8
Figure 6-8 Edit IP Static Route	6-9
Figure 7-1 Menu 11.3 — Remote Node Bridging Options	7-2
Figure 7-2 Menu 12.3.1 — Edit Bridge Static Route.....	7-3
Figure 8-1 How NAT Works	8-3
Figure 8-2 NAT Application With IP Alias	8-4
Figure 8-3 Menu 4 — Applying NAT for Internet Access	8-7
Figure 8-4 Menu 11.3 — Applying NAT to the Remote Node	8-8
Figure 8-5 Menu 15 — NAT Setup.....	8-9
Figure 8-6 Menu 15.1 — Address Mapping Sets.....	8-9
Figure 8-7 Menu 15.1.255 — SUA Address Mapping Rules.....	8-11
Figure 8-8 Menu 15.1.1 — First Set	8-12
Figure 8-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set.....	8-15
Figure 8-10 Menu 15.2 — NAT Server Setup.....	8-18

Figure 8-11 Menu 15.2.1 — NAT Server Setup	8-18
Figure 8-12 Multiple Servers Behind NAT Example.....	8-19
Figure 8-13 NAT Example 1	8-20
Figure 8-14 Menu 4 — Internet Access & NAT Example	8-21
Figure 8-15 NAT Example 2.....	8-22
Figure 8-16 Menu 15.2.1 — Specifying an Inside Server	8-23
Figure 8-17 NAT Example 3.....	8-25
Figure 8-18 Example 3: Menu 11.3	8-26
Figure 8-19 Example 3: Menu 15.1.1.1	8-26
Figure 8-20 Example 3: Final Menu 15.1.1	8-27
Figure 8-21 NAT Example 4.....	8-29
Figure 8-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule.....	8-29
Figure 8-23 Example 4: Menu 15.1.1 — Address Mapping Rules	8-30
Figure 9-1 Prestige Firewall Application.....	9-3
Figure 9-2 Three-Way Handshake	9-5
Figure 9-3 SYN Flood	9-5
Figure 9-4 Smurf Attack	9-6
Figure 9-5 Stateful Inspection.....	9-8
Figure 10-1 Menu 21 — Filter and Firewall Setup.....	10-1
Figure 10-2 Menu 21.2 — Firewall Setup.....	10-2
Figure 10-3 Example Firewall Log.....	10-2
Figure 11-1 Enabling the Firewall.....	11-2
Figure 11-2 E-mail Screen.....	11-3
Figure 11-3 E-mail Log	11-6
Figure 11-4 Attack Alert	11-8
Figure 12-1 LAN to WAN Traffic.....	12-3
Figure 12-2 WAN to LAN Traffic.....	12-4

Figure 12-3 Firewall Rules Summary — First Screen	12-5
Figure 12-4 Creating/Editing A Firewall Rule	12-10
Figure 12-5 Adding/Editing Source and Destination Addresses	12-12
Figure 12-6 Timeout Screen.....	12-13
Figure 13-1 Customized Services	13-1
Figure 13-2 Creating/Editing A Customized Service	13-3
Figure 13-3 Configure Source IP	13-5
Figure 13-4 Customized Service for Syslog.....	13-6
Figure 13-5 Syslog Rule Configuration	13-7
Figure 13-6 Example Rule Summary	13-8
Figure 14-1 Log Screen.....	14-1
Figure 16-1 Outgoing Packet Filtering Process	16-2
Figure 16-2 Filter Rule Process.....	16-3
Figure 16-4 Menu 21 — Filter and Firewall Setup.....	16-4
Figure 16-5 Menu 21.1 — Filter Set Configuration.....	16-5
Figure 16-6 NetBIOS_WAN Filter Rules Summary	16-6
Figure 16-7 NetBIOS_LAN Filter Rules Summary.....	16-6
Figure 16-8 PPPoE Filter Rules Summary.....	16-7
Figure 16-9 TEL_FTP_WEB_SNM Filter Rules Summary	16-7
Figure 16-10 Menu 21.1.7.1 — TCP/IP Filter Rule	16-10
Figure 16-11 Executing an IP Filter	16-13
Figure 16-12 Menu 21.1.5.1 — Generic Filter Rule	16-14
Figure 16-13 Protocol and Device Filter Sets	16-16
Figure 16-14 Sample Telnet Filter.....	16-17
Figure 16-15 Sample Filter — Menu 21.1.9.1	16-18
Figure 16-16 Sample Filter Rules Summary — Menu 21.1.9.....	16-19
Figure 16-17 Filtering Ethernet Traffic	16-20

Figure 16-18 Filtering Remote Node Traffic	16-22
Figure 16-19 Filtering Remote Node Traffic with PPPoE	16-22
Figure 17-1 SNMP Management Model.....	17-1
Figure 17-2 Menu 22 — SNMP Configuration	17-3
Figure 18-1 Menu 24 — System Maintenance	18-1
Figure 18-2 Menu 24.1 — System Maintenance — Status.....	18-2
Figure 18-3 Menu 24.2 — System Information and Console Port Speed.....	18-3
Figure 18-4 Menu 24.2.1 — System Maintenance — Information	18-4
Figure 18-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed.....	18-5
Figure 18-6 Menu 24.3 — System Maintenance — Log and Trace	18-5
Figure 18-7 Sample Error and Information Messages	18-6
Figure 18-8 Menu 24.3.2 — System Maintenance — Syslog and Accounting	18-6
Figure 18-9 Menu 24.4 — System Maintenance — Diagnostic	18-8
Figure 18-10 Command Mode.....	18-9
Figure 19-1 Telnet in Menu 24.5	19-3
Figure 19-2 FTP Session Example.....	19-4
Figure 19-3 System Maintenance — Backup Configuration.....	19-6
Figure 19-4 System Maintenance — Starting Xmodem Download Screen.....	19-7
Figure 19-5 Backup Configuration Example	19-7
Figure 19-6 Successful Backup Confirmation Screen	19-7
Figure 19-7 Telnet into Menu 24.6	19-8
Figure 19-8 Restore Using FTP Session Example	19-9
Figure 19-9 System Maintenance — Restore Configuration.....	19-9
Figure 19-10 System Maintenance — Starting Xmodem Download Screen.....	19-9
Figure 19-11 Restore Configuration Example	19-10
Figure 19-12 Successful Restoration Confirmation Screen	19-10
Figure 19-13 Telnet Into Menu 24.7.1 — Upload System Firmware	19-11

Figure 19-14 Telnet Into Menu 24.7.2 — System Maintenance	19-11
Figure 19-15 FTP Session Example of Firmware File Upload	19-12
Figure 19-16 Menu 24.7.1 as seen using the Console Port	19-14
Figure 19-17 Example Xmodem Upload	19-14
Figure 19-18 Menu 24.7.2 as seen using the Console Port	19-15
Figure 19-19 Example Xmodem Upload	19-16
Figure 20-1 Command Mode in Menu 24.....	20-1
Figure 20-2 Valid Commands	20-2
Figure 20-3 Call Control	20-2
Figure 20-4 Budget Management.....	20-3
Figure 20-5 Menu 24 — System Maintenance	20-4
Figure 20-6 Menu 24.10 System Maintenance — Time and Date Setting.....	20-4
Figure 21-1 Telnet Configuration on a TCP/IP Network	21-1
Figure 21-2 Menu 24.11 – Remote Management Control.....	21-3
Figure 22-1 IP Routing Policy Setup	22-2
Figure 22-2 Menu 25.1 — Sample IP Routing Policy Setup	22-3
Figure 22-3 IP Routing Policy	22-4
Figure 22-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup	22-6
Figure 22-5 Menu 11.3 — Remote Node Network Layer Options	22-6
Figure 22-6 Example of IP Policy Routing.....	22-7
Figure 22-7 IP Routing Policy Example	22-8
Figure 22-8 IP Routing Policy	22-9
Figure 22-9 Applying IP Policies	22-9
Figure 23-1 Menu 26 - Schedule Setup.....	23-1
Figure 23-2 Schedule Set Setup.....	23-2
Figure 23-3 Applying Schedule Set(s) to a Remote Node (PPPoE).....	23-4
Figure 24-1 Encryption and Decryption.....	24-2

Figure 24-2 VPN Application	24-3
Figure 24-3 IPSec Architecture.....	24-4
Figure 24-4 Transport and Tunnel Mode IPSec Encapsulation.....	24-5
Figure 25-1 VPN SMT Menu Tree	25-1
Figure 25-2 Menu 27 — VPN/IPSec Setup	25-2
Figure 25-3 IPSec Summary Fields	25-3
Figure 25-4 Telecommuter's Prestige Configuration.....	25-5
Figure 25-5 Headquarters Prestige Configuration	25-5
Figure 25-6 Menu 27.1 — IPSec Summary.....	25-6
Figure 25-7 Menu 27.1.1 — IPSec Setup	25-9
Figure 25-8 Two Phases to set up the IPSec SA	25-13
Figure 25-9 Menu 27.1.1.1 — IKE Setup.....	25-15
Figure 25-10 Menu 27.1.1.2 — Manual Setup	25-18
Figure 26-1 Menu 27.2 — SA Monitor	26-1
Figure 27-1 Example VPN Initiator IPSec Log	27-1
Figure 27-2 Example VPN Responder IPSec Log	27-2
Figure 28-1 Configuration Text File Format — Column Descriptions.....	28-2
Figure 28-2 Invalid Parameter Entered — Command Line Example.....	28-3
Figure 28-3 Valid Parameter Entered — Command Line Example.....	28-3
Figure 28-4 Internal SPTGEN FTP Download Example.....	28-3
Figure 28-5 Internal SPTGEN FTP Upload Example.....	28-4

List of Diagrams

Diagram 1 Single-PC per Router Hardware Configuration	A
Diagram 2 Prestige as a PPPoE Client.....	B
Diagram 3 Virtual Circuit Topology	C
Diagram 4 Option to Enter Debug Mode.....	D

Diagram 5 Boot Module Commands E

List of Tables

Table 2-1 Front Panel LED Description..... 2-1

Table 2-2 Main Menu Commands..... 2-11

Table 2-3 Main Menu Summary 2-12

Table 3-1 General Setup Menu Fields..... 3-2

Table 3-2 Configure Dynamic DNS Menu Fields..... 3-4

Table 4-1 IP Alias Setup Menu Fields..... 4-7

Table 4-2 DHCP Ethernet Setup Menu Fields..... 4-9

Table 4-3 TCP/IP Ethernet Setup Menu Fields 4-10

Table 4-4 Internet Account Information 4-13

Table 4-5 Internet Access Setup Menu Fields 4-16

Table 5-1 Remote Node Profile Menu Fields..... 5-4

Table 5-2 Remote Node Network Layer Options..... 5-7

Table 6-1 TCP/IP-Related Fields in Menu 11.1 — Remote Node Profile..... 6-3

Table 6-2 TCP/IP Remote Node Configuration 6-5

Table 6-3 Edit IP Static Route Menu Fields..... 6-9

Table 7-1 Remote Node Bridge Options 7-2

Table 7-2 Edit Bridge Static Route Menu Fields..... 7-3

Table 8-1 NAT Definitions..... 8-1

Table 8-2 NAT Mapping Types 8-5

Table 8-3 Applying NAT in Menus 4 & 11.3 8-8

Table 8-4 SUA Address Mapping Rules..... 8-11

Table 8-5 Fields in Menu 15.1.1 8-13

Table 8-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set..... 8-15

Table 8-7 Services & Port Numbers..... 8-16

Table 9-1 Common IP Ports 9-4

Table 9-2 ICMP Commands That Trigger Alerts 9-6

Table 9-3 Legal NetBIOS Commands.....	9-7
Table 9-4 Legal SMTP Commands	9-7
Table 10-1 View Firewall Log.....	10-3
Table 11-1 E-mail.....	11-4
Table 11-2 SMTP Error Messages.....	11-5
Table 11-3 Attack Alert.....	11-9
Table 12-1 Firewall Rules Summary — First Screen.....	12-5
Table 12-2 Predefined Services	12-7
Table 12-3 Creating/Editing A Firewall Rule	12-10
Table 12-4 Adding/Editing Source and Destination Addresses	12-12
Table 12-5 Timeout Menu	12-14
Table 13-1 Customized Services	13-2
Table 13-2 Creating/Editing A Custom Port.....	13-3
Table 14-1 Log Screen	14-2
Table 16-1 Filter Rules Summary Menu Abbreviations	16-8
Table 16-2 Rule Abbreviations Used.....	16-8
Table 16-3 TCP/IP Filter Rule Menu Fields.....	16-10
Table 16-4 Generic Filter Rule Menu Fields	16-15
Table 16-5 Filter Sets Table.....	16-20
Table 17-1 SNMP Configuration Menu Fields.....	17-3
Table 17-2 SNMP Traps	17-4
Table 17-3 Ports and Permanent Virtual Circuits	17-4
Table 18-1 System Maintenance — Status Menu Fields.....	18-2
Table 18-2 Fields in System Maintenance.....	18-4
Table 18-3 System Maintenance Menu — Syslog Parameters.....	18-7
Table 18-4 System Maintenance Menu — Diagnostic	18-9
Table 19-1 Filename Conventions.....	19-2
Table 19-2 General Commands for GUI-based FTP Clients.....	19-4

Table 19-3 General Commands for GUI-based TFTP Clients	19-6
Table 20-1 Budget Management	20-3
Table 20-2 Time and Date Setting Fields	20-5
Table 21-1 Menu 24.11 – Remote Management Control	21-3
Table 22-1 IP Routing Policy Setup	22-3
Table 22-2 IP Routing Policy	22-4
Table 23-1 Schedule Set Setup Fields	23-2
Table 24-1 VPN and NAT	24-6
Table 25-1 AH and ESP	25-3
Table 25-2 Telecommuter and Headquarters Configuration Example	25-4
Table 25-3 Menu 27.1 — IPSec Summary.....	25-6
Table 25-4 Menu 27.1.1 — IPSec Setup	25-9
Table 25-5 Menu 27.1.1.1 — IKE Setup.....	25-15
Table 25-6 Active Protocol — Encapsulation and Security Protocol.....	25-17
Table 25-7 Menu 27.1.1.2 — Manual Setup	25-18
Table 26-1 Menu 27.2 — SA Monitor	26-1
Table 27-1 Sample IKE Key Exchange Logs.....	27-2
Table 27-2 Sample IPSec Logs During Packet Transmission	27-4
Table 27-3 RFC-2408 ISAKMP Payload Types.....	27-4
Table 29-1 Troubleshooting the LAN LED.....	29-1
Table 29-2 Troubleshooting the DSL LED	29-2
Table 29-3 Troubleshooting the LAN Interface	29-2
Table 29-4 Troubleshooting the WAN Interface	29-2
Table 29-5 Troubleshooting Internet Access	29-3
Table 29-6 Troubleshooting the Password	29-3
Table 29-7 Troubleshooting the Web Configurator	29-4
Table 29-8 Troubleshooting Remote Management	29-4

Preface

Congratulations on your purchase of the Prestige 652 ADSL Router with VPN and Firewall.

There are two Prestige 652 models, one for ADSL over POTS (Plain Old Telephone System) and one for ADSL over ISDN (Integrated Synchronous Digital System). Both models are discussed together in this guide.

The Prestige 652 is an ADSL router used for Internet/LAN access via an ADSL line. The P652 can run maximum upstream transmission rates of up to 832Kbps and maximum downstream transmission rates of 8Mbps. The actual rate depends on the copper category of your telephone wire, distance from the central office and the type of ADSL service subscribed to. See the *What is DSL* section for more background information on DSL and ADSL.

The P652's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Your Prestige is easy to install and configure. All functions of the Prestige are software configurable via the SMT (System Management Terminal) and web configurator. Advanced users may configure the Prestige using CLI (Command Line Interface) commands.

Register your Prestige online at www.zyxel.com for free future product updates and information.

About This User's Guide

This User's Guide covers all aspects of the Prestige 652 operations and shows you how to use the SMT to get the best out of its multiple advanced features. It is designed to guide you through the correct configuration of your Prestige 652 for various applications.

Related Documentation

- **Supporting Disk**
More detailed information and examples can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your Prestige for Internet Access, general and advanced FAQs, Application Notes, Troubleshooting, a reference for CI Commands and bundled software.
- **Read Me First**
Our Read Me First is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- **ZyXEL Web Site and Glossary**

Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation

Syntax Conventions

- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The Prestige 652 ADSL Router with VPN and Firewall may be referred to as the P652 or the Prestige in this User’s Guide.

The following section offers some background information on DSL. Skip it if you wish to begin working with your router right away.

What is DSL?

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

What is ADSL?

It is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. As mentioned, this works well for a typical Internet session in which more information is downloaded, for example, from Web servers, than is uploaded. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.

Part I:

GETTING STARTED

This part is structured as a step-by-step guide to help you connect, install and set up your Prestige to operate on your network and to access the Internet. Described are Key Features and Applications, Hardware Installation, Initial Setup and Internet Access.

Chapter 1

Getting To Know Your Prestige

This chapter describes the key features and applications of your Prestige.

1.1 Prestige 652 ADSL Security Router

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface and a high-speed ADSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks.

The Prestige provides not only ease of installation and high-speed Internet access, but also a complete security solution. The Prestige 652 combines an ADSL router with a robust firewall and VPN capability.

The web browser-based Graphical User Interface provides easy management and is totally independent of the operating system platform you use.

1.2 Features

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

- **High Speed Internet Access**

Your Prestige can support downstream transmission rates of up to 8Mbps and upstream transmission rates of 832 Kbps. Your Prestige also supports rate management; rate management allows ADSL subscribers to select an Internet access speed that best suits their needs and budgets.

- **IPSec VPN Capability**

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The Prestige's VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

- **Firewall**

The Prestige is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Prestige firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

You can configure most features of the Prestige via SMT but we recommend you configure the firewall and content filters using the Prestige Web Configurator.

- **Content Filtering**

The Prestige can block specific URLs by using the keyword blocking feature.

- **Internal SPTGEN**

Internal SPTGEN (System Parameter Table Generator) lets you configure, save and upload multiple menus at the same time using just one configuration text file - eliminating the need to navigate and configure individual SMT menus for each Prestige.

- **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client to use this service.

- **Packet Filtering**

The Packet Filtering mechanism blocks unwanted traffic from entering/leaving your network.

- **PPPoE Support (RFC2516)**

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the Prestige is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

- **Network Address Translation (NAT)**

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network. This feature allows multiple-user Internet access for the cost of a single IP account. NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealPlayer, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

- **10/100M Auto-negotiation Ethernet/Fast Ethernet Interface**

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

- **Multiple PVC (Permanent Virtual Circuits) Support**

Your Prestige supports up to 8 PVCs.

- **ADSL Transmission Rate Standards**

- ◆ Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.
- ◆ G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.
- ◆ Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G.992.2)).
- ◆ TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ◆ ATM Forum UNI 3.1 PVC.
- ◆ Supports up to 8 PVCs (UBR, CBR).
- ◆ Multiple Protocol over AAL5 (RFC 1483).
- ◆ PPP over AAL5 (RFC 2364).
- ◆ PPP over Ethernet over AAL5 (RFC 2516).

- **Protocol Support**

- ◆ DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The Prestige can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignments from the actual DHCP server to the clients.

- ◆ IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

- ◆ IP Policy Routing (IPPR)

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

- ◆ PPP (Point-to-Point Protocol) link layer protocol.
- ◆ Transparent bridging for unsupported network layer protocols.
- ◆ RIP I/RIP II
- ◆ IGMP Proxy

- ◆ ICMP support
- ◆ IP QoS support
- ◆ MIB II support (RFC 1213)

● **Networking Compatibility**

Your Prestige is compatible with the major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

● **Multiplexing**

The Prestige supports VC-based and LLC-based multiplexing.

● **Encapsulation**

The Prestige supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing as well as PPP over Ethernet (RFC 2516).

Network Management

- ◆ Menu driven SMT (System Management Terminal) management
- ◆ Embedded Web Configurator
- ◆ CLI (Command Line Interpreter)
- ◆ Remote SMT session via Telnet
- ◆ SNMP manageable
- ◆ Local SMT session via console port
- ◆ DHCP Server/Client
- ◆ Built-in Diagnostic Tools
- ◆ Syslog
- ◆ Telnet Support (Password-protected telnet access to internal configuration manager)
- ◆ TFTP/FTP server, firmware upgrade and configuration backup/support supported
- ◆ Supports OAM F4/F5 loop-back, AIS and RDI OAM cells

● **Other PPPoE Features**

- ◆ PPPoE idle time out
- ◆ PPPoE Dial on Demand

- **Diagnostics Capabilities**

- ◆ The Prestige can perform self-diagnostic tests. These tests check the integrity of the following circuitry:
 - ◆ FLASH memory
 - ◆ ADSL circuitry
 - ◆ RAM
 - ◆ LAN port

- **Ease of Installation**

Your Prestige is designed for quick, intuitive and easy installation.

- **Housing**

Your Prestige's all new compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

1.3 Applications for the Prestige 652

1.3.1 Internet Access

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. A typical Internet Access application is shown below.

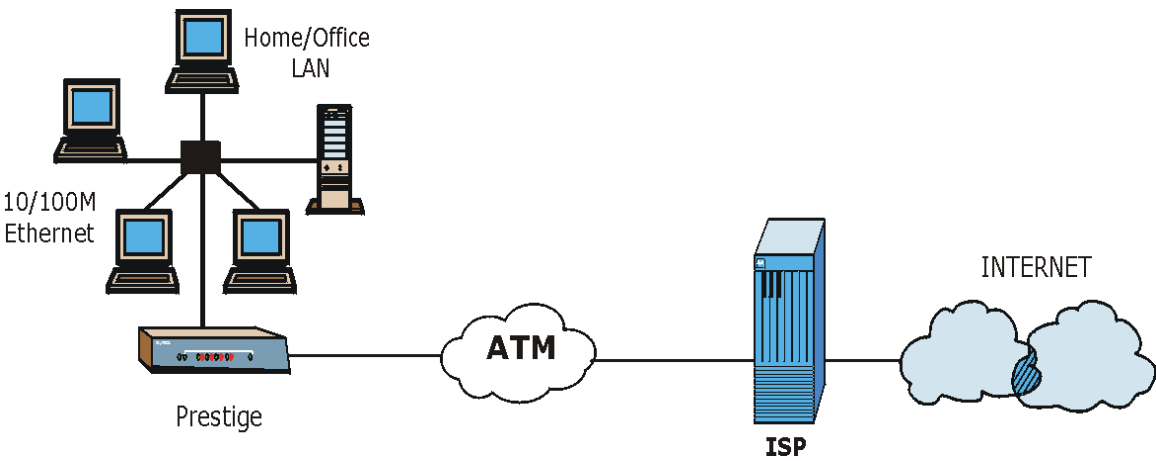


Figure 1-1 Internet Access Application

Internet Single User Account

For a SOHO (Small Office/Home Office) environment, your Prestige offers the Network Address Translation (NAT) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address.

1.3.2 Firewall for Secure Broadband Internet Access

The Prestige provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

Private
LAN

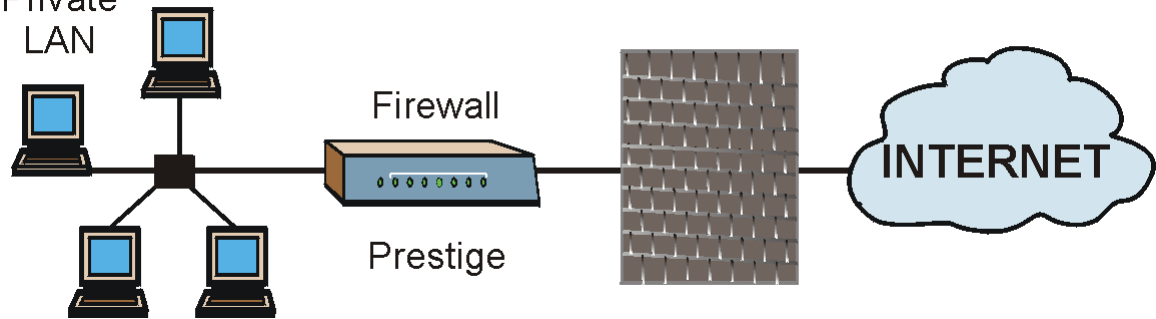


Figure 1-2 Firewall Application

1.3.3 LAN to LAN Application

You can use the Prestige to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application for your Prestige is shown as follows.

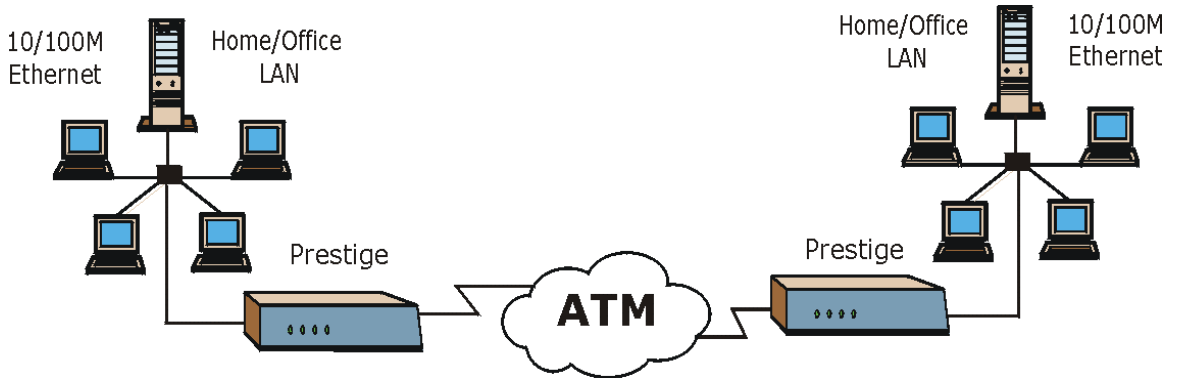


Figure 1-3 LAN-to-LAN Application

1.3.4 VPN Application

The Prestige's VPN feature makes it an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) for leased lines between sites. VPN ensures the privacy and integrity of your data transmissions.

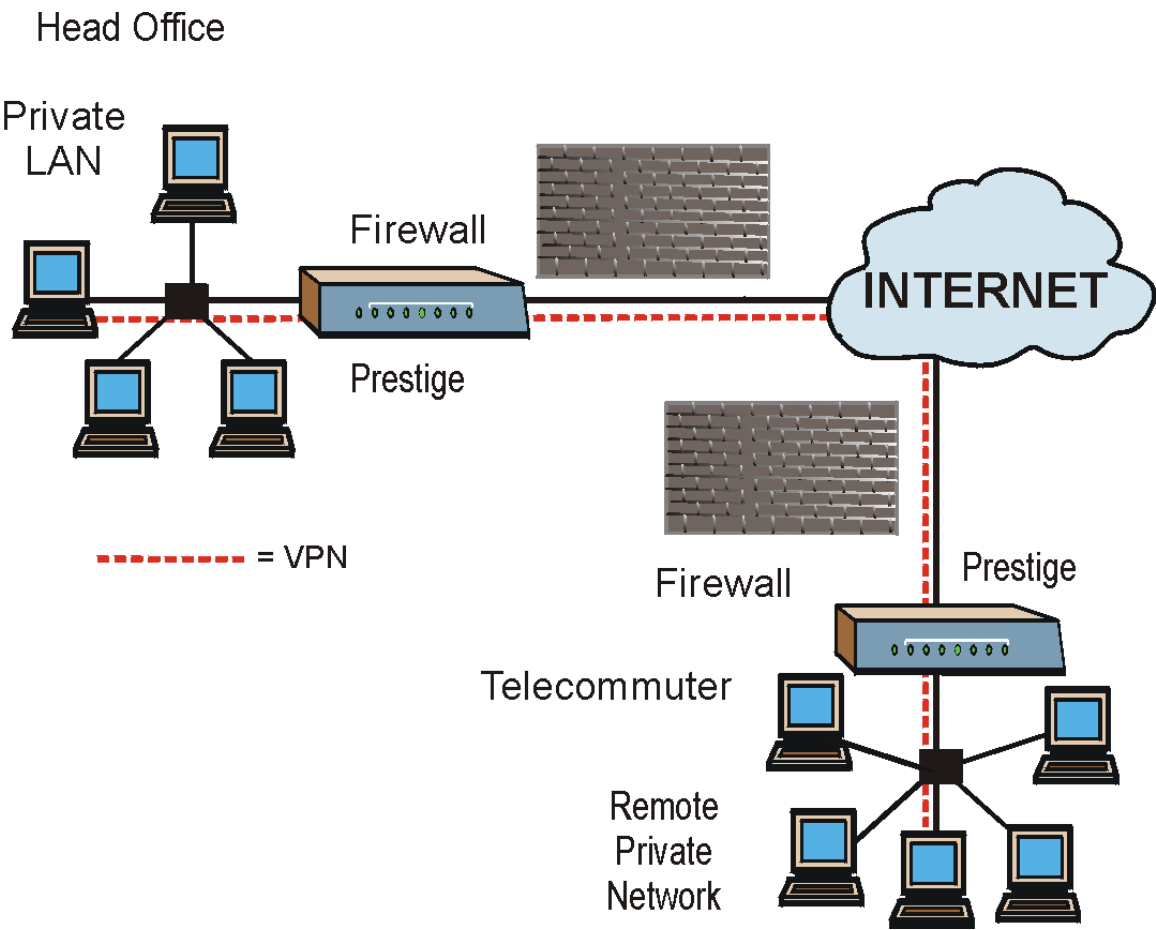


Figure 1-4 VPN Application

Chapter 2

Hardware Installation and Initial Setup

This chapter describes the physical features of the Prestige and how to make cable connections.

2.1 Front Panel LEDs of the P652

The LEDs on the front panel indicate the operational status of your Prestige

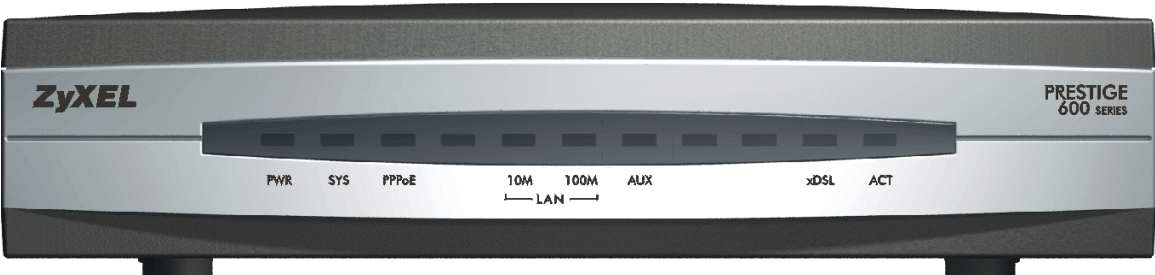


Figure 2-1 Front Panel

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Prestige is receiving power.
		Blinking	The Prestige is performing a self-test.
		Off	The Prestige is not receiving power.
SYS	Green	On	The Prestige is functioning properly.
		Blinking	The Prestige is rebooting.
		Off	The Prestige is not ready or has malfunctioned.
	Red	On	The Prestige is not receiving enough power.
PPPoE	Green	On	The Prestige is connected to the PPPoE server.
		Off	There is no connection to the PPPoE server.

LED	COLOR	STATUS	DESCRIPTION
LAN 10M	Green	On	The Prestige has a successful 10Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have a 10Mb Ethernet connection.
LAN 100M	Orange	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The Prestige does not have a 100Mb Ethernet connection.
AUX	This LED is reserved for a feature to be available in the future.		
xDSL	Green	On	The Prestige is linked successfully to a DSLAM.
		Blinking	The Prestige is initializing or sending/receiving data.
		Off	The DSL link is down.
ACT	Green	On	The Prestige has a successful Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The system is not ready or has malfunctioned.

2.2 Rear Panel and Connections

The following figure shows the rear panel of your Prestige.



Figure 2-2 Rear Panel

2.2.1 xDSL Port

Connect the Prestige directly to the wall jack using a DSL cable (telephone wire). Connect a microfilter(s) between the wall jack and your telephone(s). A microfilter acts as low-pass filter (voice transmission takes place in the 0 to 4KHz bandwidth) and is an optional purchase.

2.2.2 Console Port

Use terminal emulator software on a computer for configuring your Prestige via console port. Connect the 9-pin end of the console cable to the console port of the Prestige and the other end (choice of 9-pin or 25-pin, depending on your computer) end to a serial port (COM1, COM2 or other COM port) of your computer. You can use an extension RS-232 cable if the enclosed one is too short. After the initial setup, you can modify the configuration remotely through telnet connections.

2.2.3 LAN 10/100M Port

For a single computer, connect the 10/100M LAN port on the Prestige to the Network Adapter on the computer using a crossover Ethernet cable with the **UPLINK** button “off” (out). Use a straight-through cable if the **UPLINK** button is “on” (in).

If you have more than one computer, then you must use an external hub. Connect the 10/100M LAN port on the Prestige to a port on the hub using a straight-through Ethernet cable and make sure the Uplink button is "on".

The corresponding LAN LED on the front panel turns on when the Prestige is on and properly connected to a computer or hub.

2.2.4 Power Port

Connect the power adapter to the port labeled POWER on the rear panel of your Prestige.

Make sure you use the correct power adapter to avoid damage to the Prestige. Refer to the *Power Adapter Specification Appendix* for this information.

2.2.5 Reset Button

Refer to section 2.8 for information on the RESET button.

2.3 Additional Installation Requirements

- A computer with an Ethernet 10Base-T/100Base-T NIC (Network Interface Card).

- A computer equipped with communications software (for example, Hyper Terminal in Windows 95) configured to the following parameters:
 - VT100 terminal emulation.
 - 9600 baud rate.
 - Parity set to none, 8 data bits, 1 stop bit.
 - Flow control set to none.

After the Prestige has been successfully connected to your network, you can make future changes to the configuration via Telnet.

2.4 P652 with POTS

2.4.1 Connecting a POTS Splitter

One major difference between Full Rate (G.dmt) ADSL and dial-up modems is the optional telephone splitter. This device keeps the telephone and ADSL signals separated, giving them the capability to provide simultaneous Internet access and telephone service on the same line. Splitters also eliminate the destructive interference conditions caused by telephone sets. The purchase of a POTS splitter is optional.

Noise generated from a telephone in the same frequency range, as the ADSL signal can be disruptive to the ADSL signal. In addition the impedance of a telephone when off-hook may be so low that it shunts the strength of the ADSL signal. When a POTS splitter is installed at the entry point, where the line comes into the home, it will filter the telephone signals before combining the ADSL and telephone signals transmitted and received. The issues of noise and impedance are eliminated with a single POTS splitter installation.

A telephone splitter is easy to install as shown in the following figure.

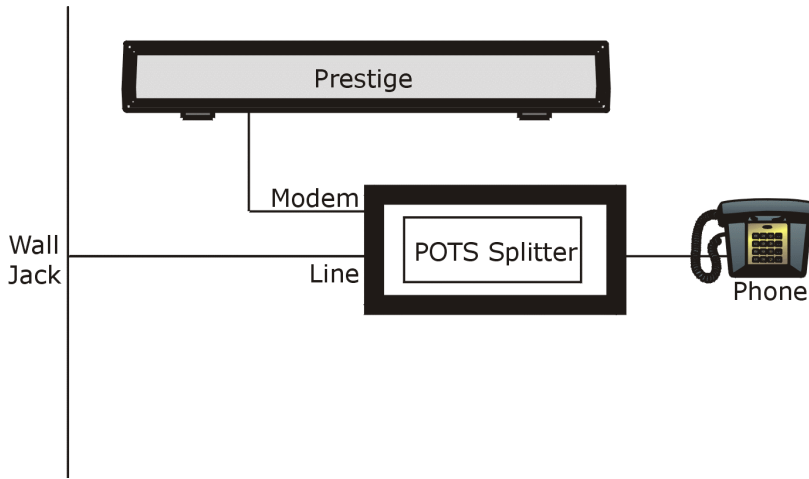


Figure 2-3 Connecting a POTS Splitter

- Step 1.** Connect the side labeled “Phone” to your telephone.
- Step 2.** Connect the side labeled “Modem” to your Prestige.
- Step 3.** Connect the side labeled “Line” to the telephone wall jack.

2.4.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The purchase of a telephone microfilter is optional.

- Step 1.** Connect a phone cable from the wall jack to the single jack end of the Y- Connector.
- Step 2.** Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.
- Step 3.** Connect another cable from the double jack end of the Y-Connector to the Prestige.
- Step 4.** Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

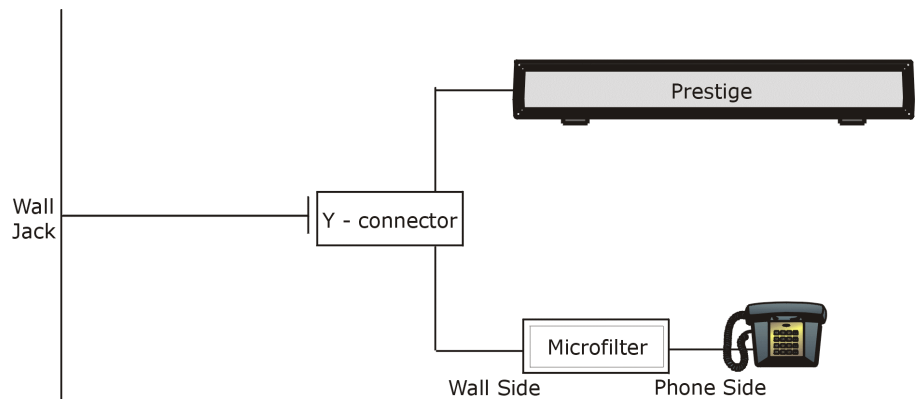


Figure 2-4 Connecting a Microfilter

2.5 P652 with ISDN

This section relates to people who use their P652 with ADSL over ISDN (digital telephone service) only. The following is an example installation for the P652 with ISDN.

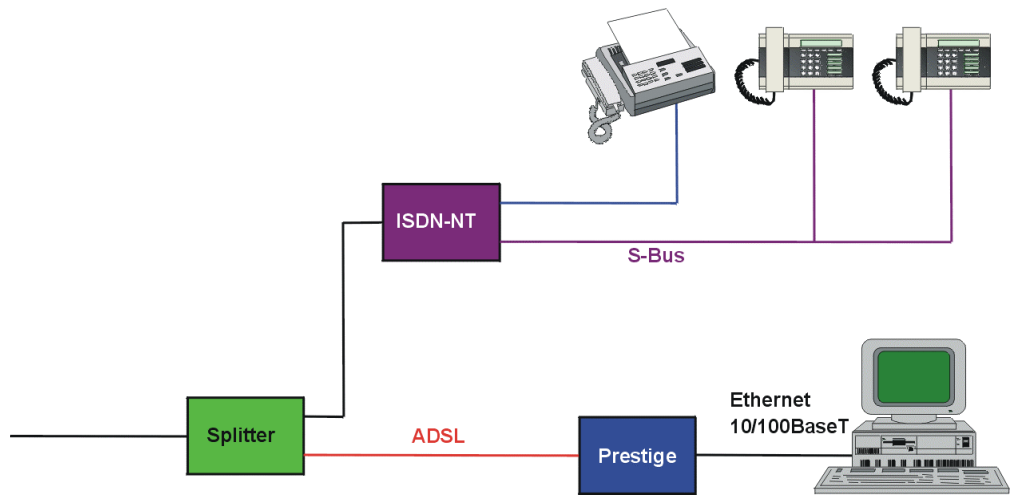


Figure 2-5 P652 with ISDN

2.6 Turning On Your Prestige

At this point, you should have connected the DSL, LAN 10/100M, console and power ports to the appropriate devices. Make sure the power adapter is plugged into an appropriate power source and the power button (located on the back of your Prestige) is “on” (pushed in).

2.7 Configuring Your Prestige For Internet Access

Configure your Prestige for Internet access using:

- Web configurator (refer to the *Read Me First* for access instructions)
- SMT (System Management Terminal). Access the SMT via:
 - LAN or WAN using Telnet
 - Console port using terminal emulation software

The remainder of this User’s Guide shows you how to configure the Prestige using SMT screens.

2.7.1 Initial Screen

When you turn on your Prestige, it performs several internal tests as well as line initialization. After the initialization, the Prestige asks you to press [ENTER] to continue, as shown.

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.  
Initialize ch = 0, ethernet address: 00:a0:c5:01:23:45  
Wan Channel init ..... done  
Loading ADSL modem F/W  
..... done  
Press ENTER to continue...
```

Figure 2-6 Power-On Display

2.7.2 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige automatically logs you out and displays a blank screen. If you see a blank screen, press [ENTER] to display the login screen again.

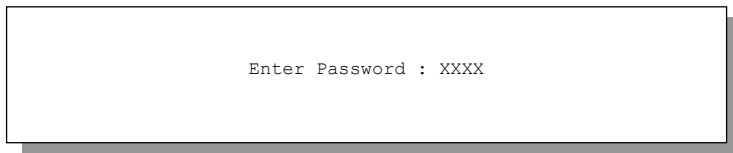


Figure 2-7 Login Screen

2.8 Resetting the Prestige

If you forget your password or cannot access the Prestige, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to “1234” and the LAN IP address to 192.168.1.1also.

To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder. Turn the Prestige off and then on to begin a session. When you turn on the Prestige again you will see the initial screen. When you see the message “Press any key to enter Debug Mode within 3 seconds” press any key to enter debug mode.

To upload the configuration file, do the following:

1. Type `atlc` after the `Enter Debug Mode` message.
2. Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.
3. After a successful firmware upload, type `atgo` to restart the Prestige.

The Prestige is now reinitialized with a default configuration file including the default password of “1234”.

2.8.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

- a. Upload the default configuration file via the console port as described above. See later in this User’s Guide for more information on how to transfer the configuration file to your Prestige using the SMT menus.
- b. Use the **RESET** button on the rear panel of the Prestige (see the next section). Use this method for cases when the password or IP address of the Prestige is not known.
- c. Use the web configurator to restore defaults (see the web configurator HTML help).

2.8.2 Procedure To Use The Reset Button

Make sure the **SYS** led is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, then release it. If the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.
2. Turn the Prestige off.
3. While pressing the **RESET** button, turn the Prestige on.
4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the Prestige is now restarting.

Release the **RESET** button and wait for the Prestige to finish restarting.

2.8.3 Prestige 652 SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

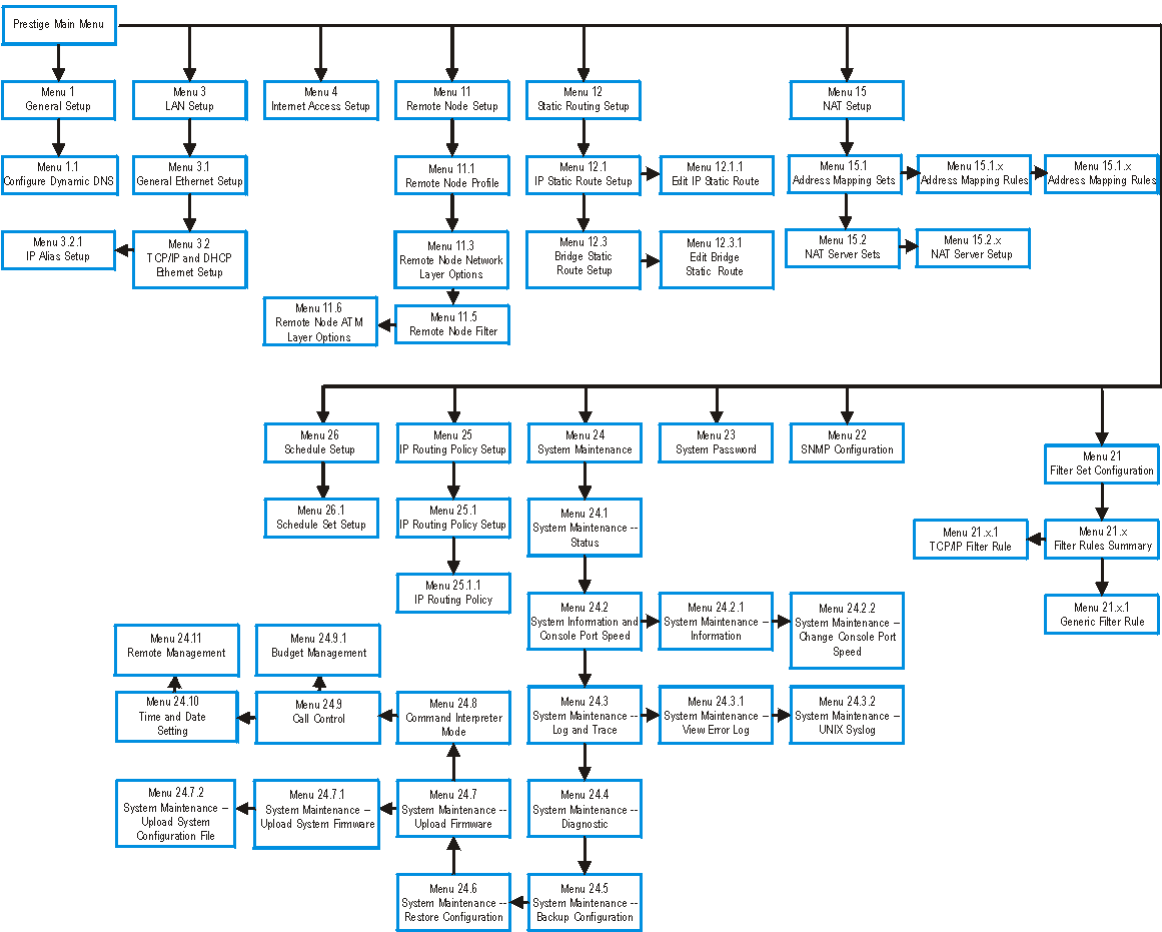


Figure 2-8 SMT Menu Overview

2.9 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 2-2 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of No . Press [SPACE BAR] once to change No to Yes , then press [ENTER] to go to the “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

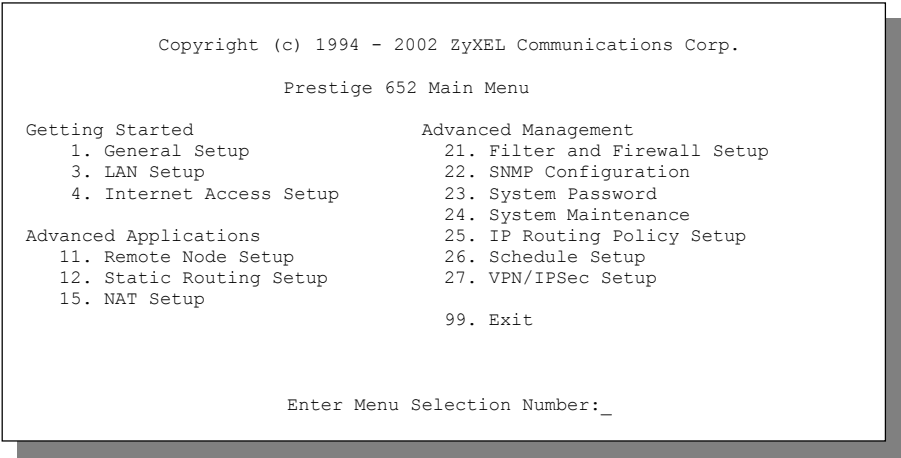


Figure 2-9 SMT Main Menu

2.9.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.

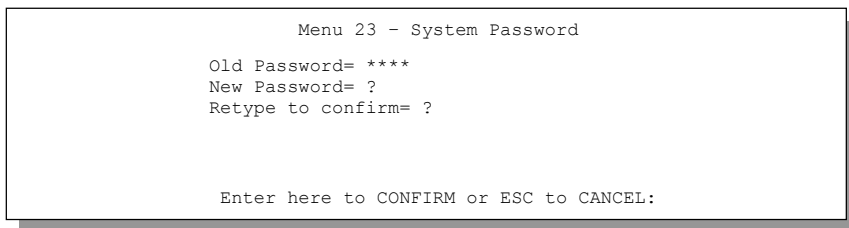
#	MENU TITLE	DESCRIPTION
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/ IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this to exit from SMT and return to a blank screen.

2.10 Changing the System Password

Change the Prestige default password by following the steps shown next.

Step 1. Enter 23 in the main menu to display **Menu 23 - System Password** as shown next.

Step 2. Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER].



```
Menu 23 - System Password

Old Password= ****
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 2-10 Menu 23 — System Password

Step 3. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

Step 4. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “X” for each character you type.

Chapter 3

General Setup

Menu 1 - General Setup contains administrative and system-related information.

3.1 System Name

System Name is for identification purposes. ZyXEL recommends you enter your computer's "Computer name".

- In Windows 95/98 click **Start -> Settings -> Control Panel** and then double-click **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows 2000 click **Start->Settings->Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows XP, click **start -> My Computer -> View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this field blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (**System Name**) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

3.2 Dynamic DNS

Dynamic DNS (Domain Name System) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in *NetMeeting*, *CU-SeeMe* or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, *myhost.dhs.org*, where *myhost* is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name.

To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The Prestige supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

3.2.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`. This feature is useful if you want to be able to use for example, `www.yourhost.dyndns.org` and still reach your hostname.

3.3 General Setup

To enter menu 1 and fill in the required information, follow these steps:

- Step 1.** Enter 1 in main menu to display **Menu 1 – General Setup**.
- Step 2.** The **Menu 1 - General Setup** screen appears, as shown next. Fill in the fields, as explained in the following table.

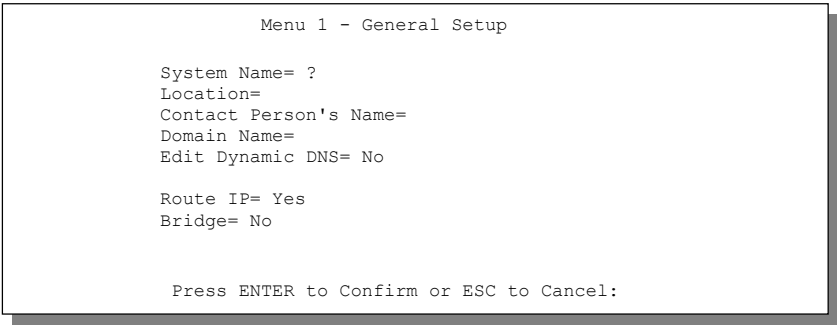


Figure 3-1 Menu 1 — General Setup

Table 3-1 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name (required)	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	P652
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe

Domain Name	Enter your domain name here (if you have one). If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. If you want to clear this field just press [SPACE BAR] and then [ENTER]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select Yes or No (default). Select Yes to configure Menu 1.1 — Configure Dynamic DNS discussed next.	No (default)
Route IP	Set this field to Yes to enable or No to disable IP routing. You must enable IP routing for Internet access.	Yes
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous Route IP field. Select Yes to turn bridging on; select No to turn bridging off.	No

3.3.1 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 — General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next).

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
Host=
EMAIL=
USER=
Password= *****
Enable Wildcard= No

Press ENTER to confirm or ESC to cancel:

```

Figure 3-2 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 3-2 Configure Dynamic DNS Menu Fields

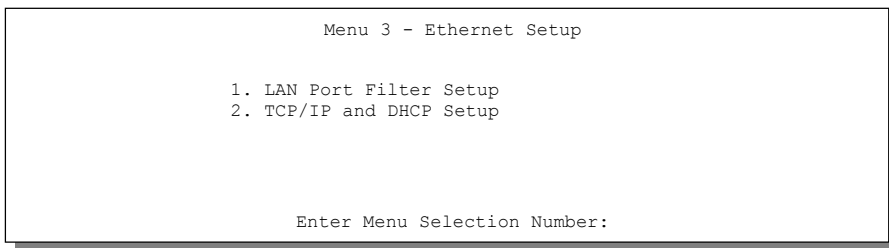
FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select Yes and then press [ENTER] to enable dynamic DNS.	Yes
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select Yes or No This field is N/A when you choose DDNS client as your service provider.	No
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

The IP address will be updated when you reconfigure menu 1 or perform DHCP client renewal.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

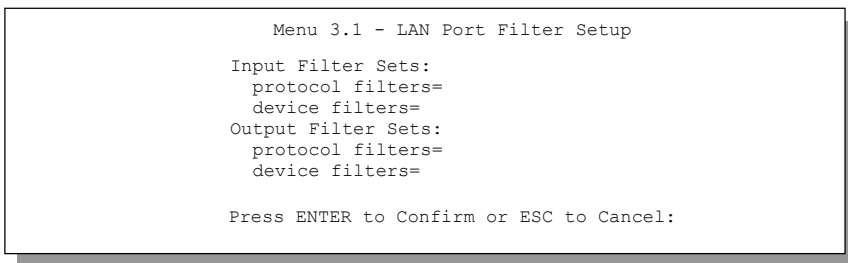
3.4 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter 3 to display menu 3.

**Figure 3-3 Menu 3 — Ethernet Setup**

3.4.1 LAN Port Filter Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

**Figure 3-4 Menu 3.1 — LAN Port Filter Setup**

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

3.5 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined next.

- For TCP/IP Ethernet setup refer to *Internet Access Application*.
- For bridging Ethernet setup refer to *Bridging Setup*.

Chapter 4

Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

4.1 Factory Ethernet Defaults

The Ethernet parameters of the Prestige are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to *TCP/IP Ethernet Setup and DHCP* to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). Please read on if you wish to change the factory defaults or to learn more about TCP/IP.

4.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

4.2.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:

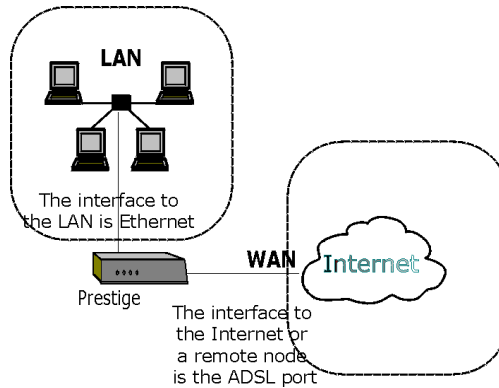


Figure 4-1 LAN & WAN IPs

4.3 TCP/IP Parameters

4.3.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

4.3.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

4.3.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both** - the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only** - the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only** - the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None** - the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

4.3.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, for instance, left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

4.4 IP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everybody on the network). Multicast is a third way to deliver IP packets to *a group* of hosts on the network - not everybody.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP Multicasting can be enabled/disabled on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

4.5 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see *IP Policy Routing*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

4.6 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

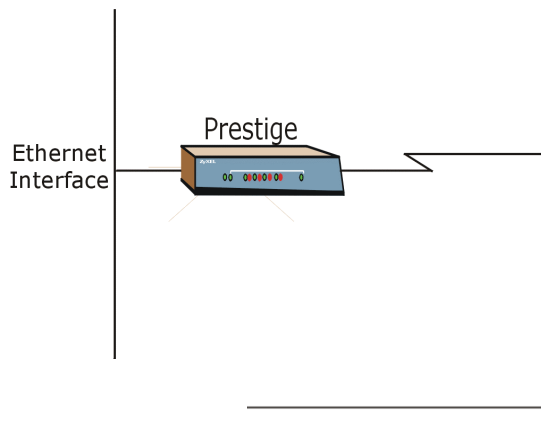


Figure 4-2 Physical Network

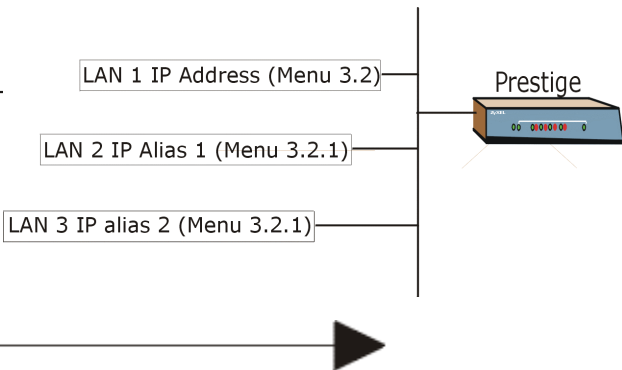


Figure 4-3 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

4.6.1 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= N/A
Multicast= None
IP Policies=
Edit IP Alias= No

Press ENTER to confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 4-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Pressing [ENTER] displays **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 4-5 Menu 3.2.1 — IP Alias Setup

Follow the instructions in the following table to configure IP Alias parameters.

Table 4-1 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias (1 or 2)	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are None , Both , In Only or Out Only .	None
Version	Press [SPACE BAR] to select the RIP version. Choices are RIP-1 , RIP-2B or RIP-2M .	RIP-1
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

4.7 Route IP Setup

The first step is to enable the IP routing in **Menu 1 - General Setup**.

To edit menu 1, type in 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

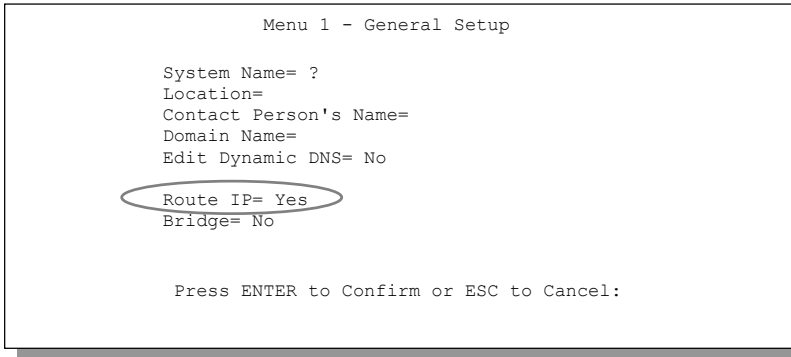


Figure 4-6 Menu 1 — General Setup

4.8 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 - Ethernet Setup**. When menu 3 appears, enter 2 to display **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next:

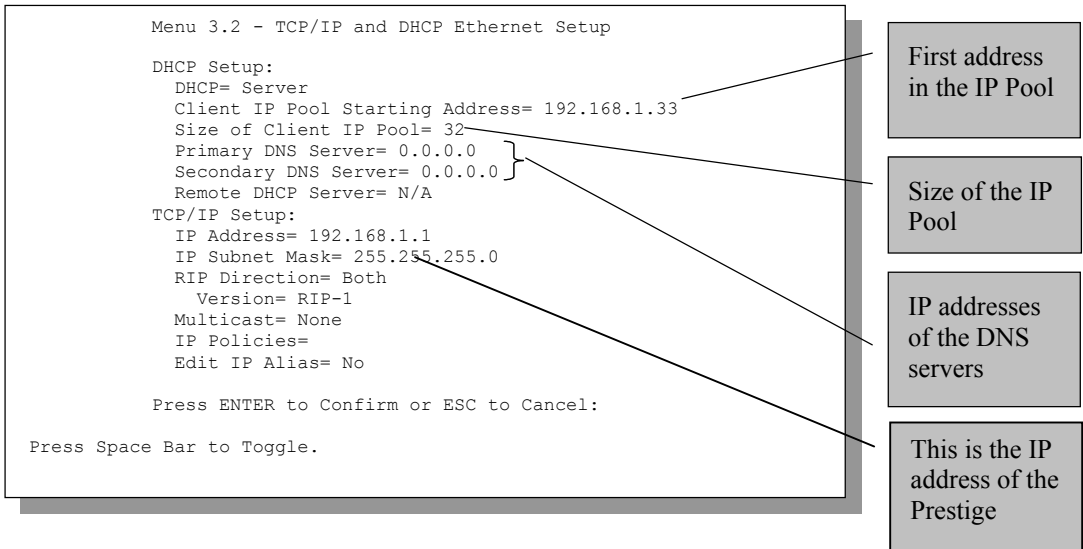


Figure 4-7 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Follow the instructions in the following table on how to configure the DHCP fields.

Table 4-2 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup	<p>DHCP If set to Server, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to None, the DHCP server will be disabled. If set to Relay, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case.</p> <p>When DHCP is used, the following items need to be set:</p>	Server (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32

FIELD	DESCRIPTION	EXAMPLE
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 4-3 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are Both , In Only , Out Only or None .	Both (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are RIP-1 , RIP-2B or RIP-2M .	RIP-1 (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press the [SPACE BAR] to enable IP Multicasting or select None to disable it.	None (default)
IP Policies	Create policies using SMT menu 25 (see the <i>IP Policy Routing chapter</i>) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change No to Yes and press [ENTER] to for menu 3.2.1	No (default)
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

4.9 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers supplied by your telephone company. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the Appendices for more information.

4.10 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

4.10.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

4.10.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

4.11 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods.

4.11.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment for instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Ethernet Encapsulation Gateway** field in menu 4 and in the **Rem IP Addr** field in menu 11.1. You can get this information from your ISP.

4.11.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the Appendices.

4.11.3 PPPoA

Please refer to RFC 2364 for more information on PPP over ATM Adaptation Layer 5 (AAL5). Refer to RFC 1661 for more information on PPP.

4.11.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

4.12 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP Address and ENET ENCAP Gateway.

4.12.1 Using PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the IP Address and ENET ENCAP Gateway fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the IP Address field and *not* the ENET ENCAP Gateway field.

4.12.2 Using RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above.

4.12.3 Using ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the IP Address and ENET ENCAP Gateway fields as supplied by your ISP. However for a dynamic IP, the Prestige acts as a

DHCP client on the WAN port and so the IP Address and ENET ENCAP Gateway fields are not applicable (N/A) as they are assigned to the Prestige by the DHCP server.

4.13 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

Table 4-4 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
System Name	Name of the Prestige (optional).	
Service Name (PPPoE Encapsulation)	Enter the PPPoE service name if the ISP supplies one. Enter “any” if the ISP does not assign you one.	
Encapsulation	PPPoE, RFC1483, PPPoA or ENET ENCAP.	
Multiplexing	LLC-based or VC-based. If this information is not given, use the default.	
VPI	Enter your Virtual Path Identifier here.	
VCI	Enter your Virtual Channel Identifier here.	
My Login	Enter the login name assigned by your ISP (for PPP/PPPoE only).	
My Password	Enter the password associated with your ISP assigned My Login (for PPPoA/PPPoE only).	
Idle Timeout (PPPoE or PPP)	Enter the time lapse, in seconds, before you automatically disconnect from the PPPoE or PPP server.	
IP Address	Enter if your IP address if it is not dynamically assigned.	
Network Address Translation	Full Feature, SUA Only or None.	

FIELD	DESCRIPTION	YOUR INFO
DNS Server Address Assignment	Primary DNS server Secondary DNS server Enter when using RFC 1483 Encapsulation or a static IP address.	
ENET ENCAP Gateway	IP Address Gateway IP Address Enter when using ENET ENCAP Encapsulation.	

4.13.1 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and “burstiness” or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of “0”, the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

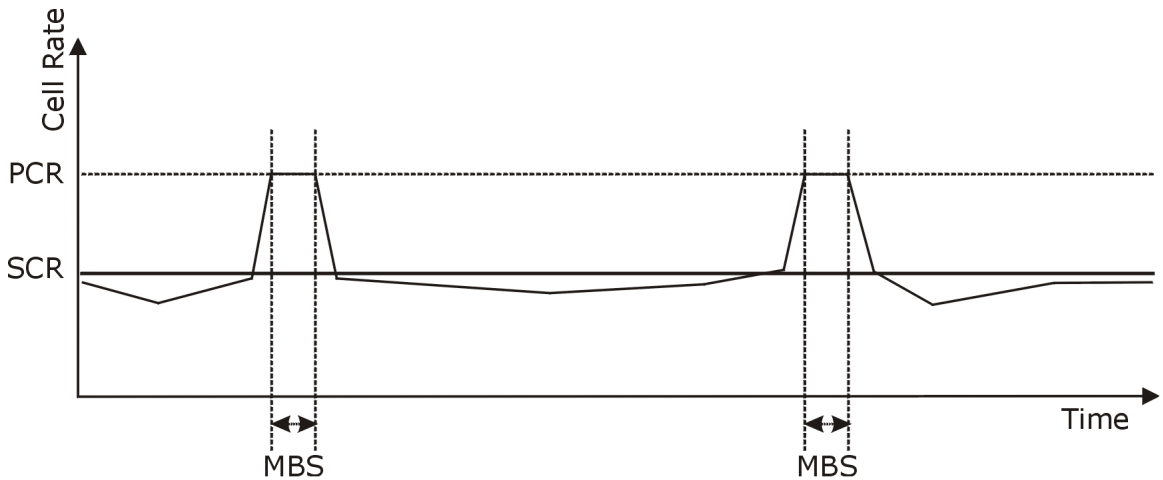


Figure 4-8 Example of Traffic Shaping

From the main menu, enter 4 to display **Menu 4 - Internet Access Setup**, (shown next).

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= RFC 1483
Multiplexing= VC-based
VPI #= 8
VCI #= 35
ATM QoS Type= CBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
IP Address= 0.0.0.0
Network Address Translation= SUA Only
Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 4-9 Internet Access Setup

The following table contains instructions on how to configure your Prestige for Internet access.

Table 4-5 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	ChangeMe
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are PPPoE , PPPoA , RFC 1483 or ENET ENCAP .	RFC 1483
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are VC-based or LLC-based .	VC-based
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	35
ATM QoS Type	Press [SPACE BAR] and select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail.	UBR
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR; it must be less than the PCR.	0
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the My Login and My Password fields for PPP and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation, then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using ENET ENCAP encapsulation.	N/A
IP Address Assignment	Press [SPACE BAR] to select Static or Dynamic address assignment.	Static
IP Address	Enter the IP address supplied by your ISP if applicable.	0.0.0.0

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation	Press [SPACE BAR] to select None , SUA Only or Full Feature . Please see the <i>NAT Chapter</i> for more details on the SUA (Single User Account) feature.	SUA Only
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See the <i>NAT</i> chapter for details.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Part II:

ADVANCED APPLICATIONS

This part shows how to configure Remote Nodes, Remote Node TCP/IP and NAT.

Chapter 5

Remote Node Configuration

This chapter covers the parameters that are protocol-independent. Protocol-dependent configuration (TCP/IP and Bridging) is covered in the following chapters.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

5.1 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

5.1.1 Remote Node Profile

To configure a remote node, follow these steps:

- Step 1.** From the main menu, enter 11 to display **Menu 11 - Remote Node Setup**.
- Step 2.** When menu 11 appears, as shown in the following figure, enter the number of the remote node that you want to configure.

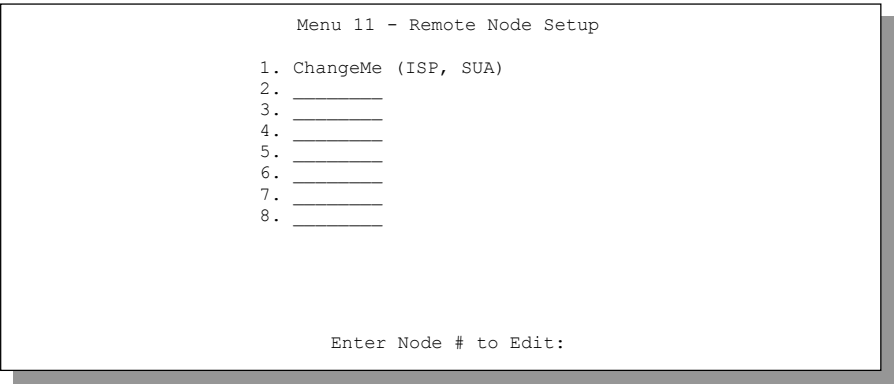


Figure 5-1 Menu 11 — Remote Node Setup

5.1.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

Scenario 3. Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

Nailed-Up Connection (PPPoA)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

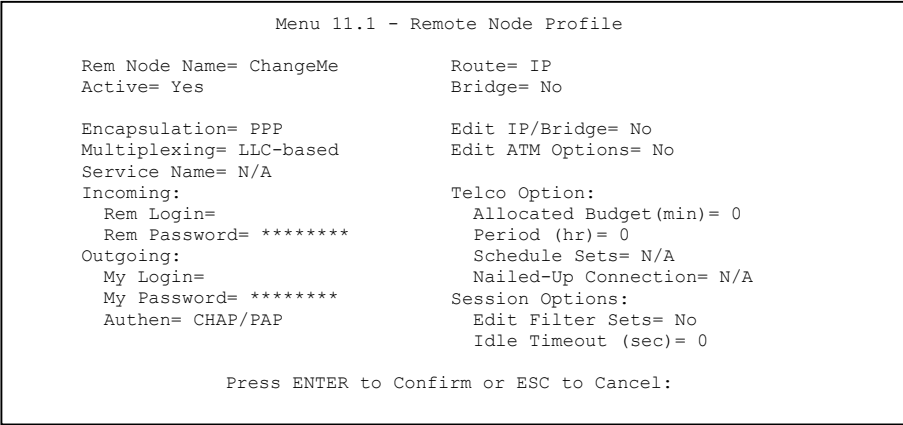


Figure 5-2 Menu 11.1 — Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 5-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	ChangeMe
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate this node. Inactive nodes are displayed with a minus sign “-”.	Yes
Encapsulation	RFC-1483 is the default configuration, press [SPACE BAR] and then [ENTER] to select either PPPoE , PPPoA (RFC-2364, PPP Encapsulation over ATM Adaptation Layer 5) or ENET ENCAP . PPPoA refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). PPPoE refers to RFC-2364 (Point-to-Point Protocol over Ethernet). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) or ENET ENCAP is selected, then the Rem Login , Rem Password , My Login , My Password , Telco Options and Idle Timeout fields are not applicable (N/A).	PPPoA
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either VC-based or LLC-based .	LLC-based

FIELD	DESCRIPTION	EXAMPLE
Service Name	When using PPPoE encapsulation, type the name of your PPPoE service here.	N/A
Incoming: Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the Rem Password will be used to authenticate this node.	
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing: My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	<p>This field sets the authentication protocol used for outgoing calls. Options for this field are:</p> <p>CHAP/PAP – Your Prestige will accept either CHAP or PAP when requested by this remote node.</p> <p>CHAP – accept CHAP (Challenge Handshake Authentication Protocol) only.</p> <p>PAP – accept PAP (Password Authentication Protocol) only.</p>	PAP
Route	This field determines the protocol used in routing. Options are IP and None .	IP
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select Yes to enable and No to disable.	No
Edit IP/Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.3 – Remote Node Network Layer Options .	No
Edit ATM Options	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.6 – Remote Node ATM Layer Options .	No
Telco Option Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the Allocated Budget is (10 minutes) and the Period (hr) is 1 (hour).	0 (default)

FIELD	DESCRIPTION	EXAMPLE
Schedule Sets	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Edit Filter Sets	Use [SPACE BAR] to choose Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	No (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	0 (default)
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.1.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

5.2 Remote Node Setup

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

- Step 1.** In menu 11.1, make sure **IP** is among the protocols in the **Route** field.
- Step 2.** Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes**, then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.

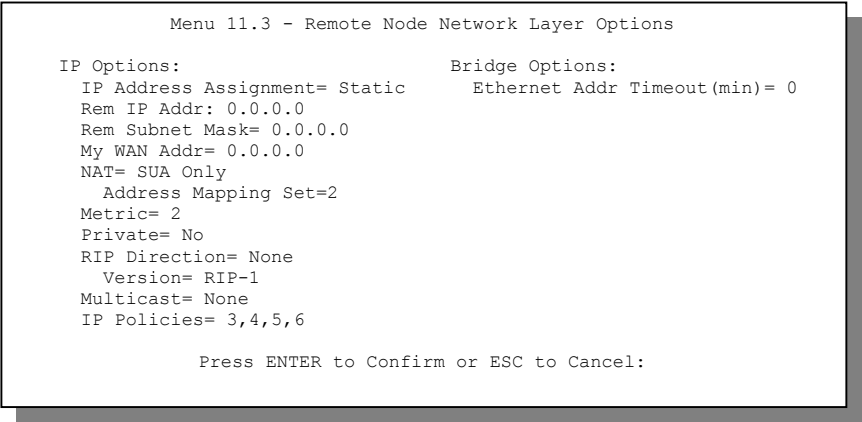


Figure 5-3 Remote Node Network Layer Options

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 5-2 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic if the remote node is using a dynamically assigned IP address, or Static if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to Static .	Static
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.	
NAT (Network Address Translation)	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige. Select SUA Only if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section 8.3.1). Select None to disable NAT.	SUA Only
Address	When Full Feature is selected in the NAT field, configure address	2

FIELD	DESCRIPTION	EXAMPLE
Mapping Set	mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the <i>NAT</i> chapter for details) and type that number here. When SUA Only is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the <i>NAT</i> chapter for details).	
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	No
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are Both , In Only , Out Only or None .	None
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are RIP-1 , RIP-2B or RIP-2M .	RIP-1
Multicast	IGMP-v1 sets IGMP to version 1, IGMP-v2 sets IGMP to version 2 and None disables IGMP.	None
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the <i>IP Policy Routing</i> chapter) and then apply them here.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.3 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. Include this in the call filter sets (call protocol filter = 1) when using PPPoE if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 5-4 Menu 11.5 — Remote Node Filter

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  Device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  Device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 5-5 Menu 11.5 — Remote Node Filter (PPPoE or PPP Encapsulation)

Chapter 6

Remote Node TCP/IP Configuration

This chapter shows a sample LAN-to-LAN application and how to configure TCP/IP remote node.

6.1 TCP/IP Configuration

The following sections describe how to configure the TCP/IP parameters of a remote node.

6.1.1 Editing TCP/IP Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on which encapsulation type you use and whether you chose **VC-based** or **LLC-based** multiplexing in menu 11.1.

VC-based Multiplexing

For **RFC-1483** or **ENET ENCAP** encapsulation with **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

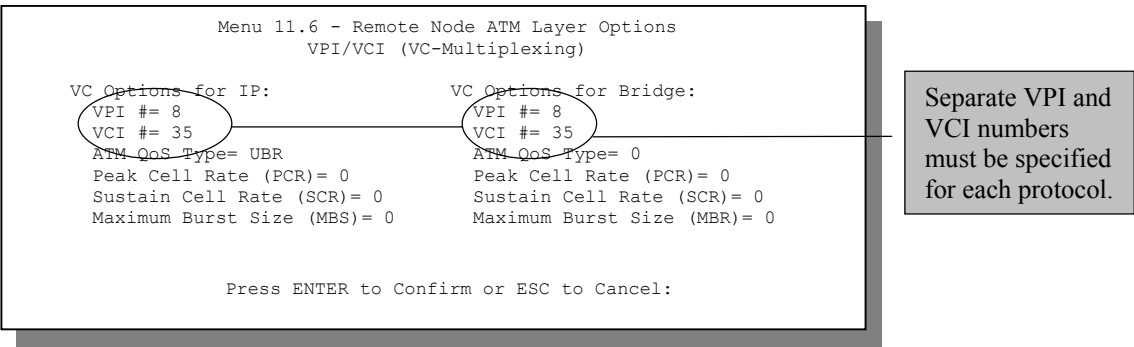


Figure 6-1 Menu 11.6 for RFC-1483 or ENET ENCAP with VC-based Multiplexing

LLC-based Multiplexing or PPPoA or PPPoE Encapsulation

For **LLC-based** multiplexing or **PPP** or **PPPoE** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

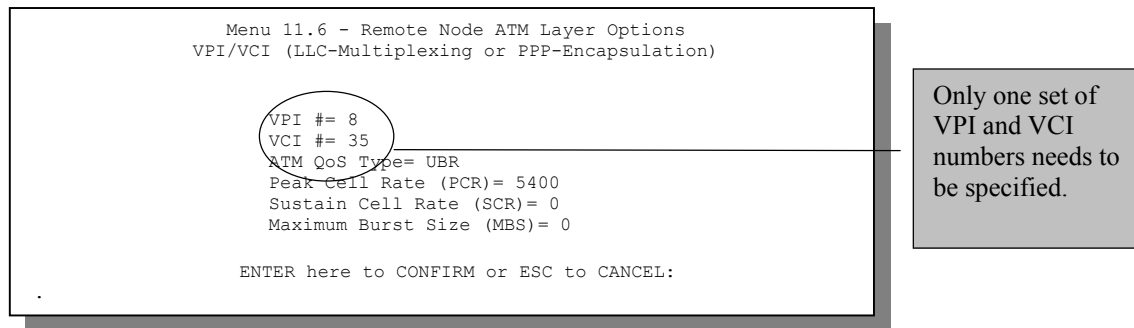


Figure 6-2 Menu 11.6 for LLC-based Multiplexing or PPPoA or PPPoE Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

The following figure uses sample IP addresses to help you understand the field of **My Wan Addr** in menu 11.3. Refer to the previous figure *LAN and WAN IPs* for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

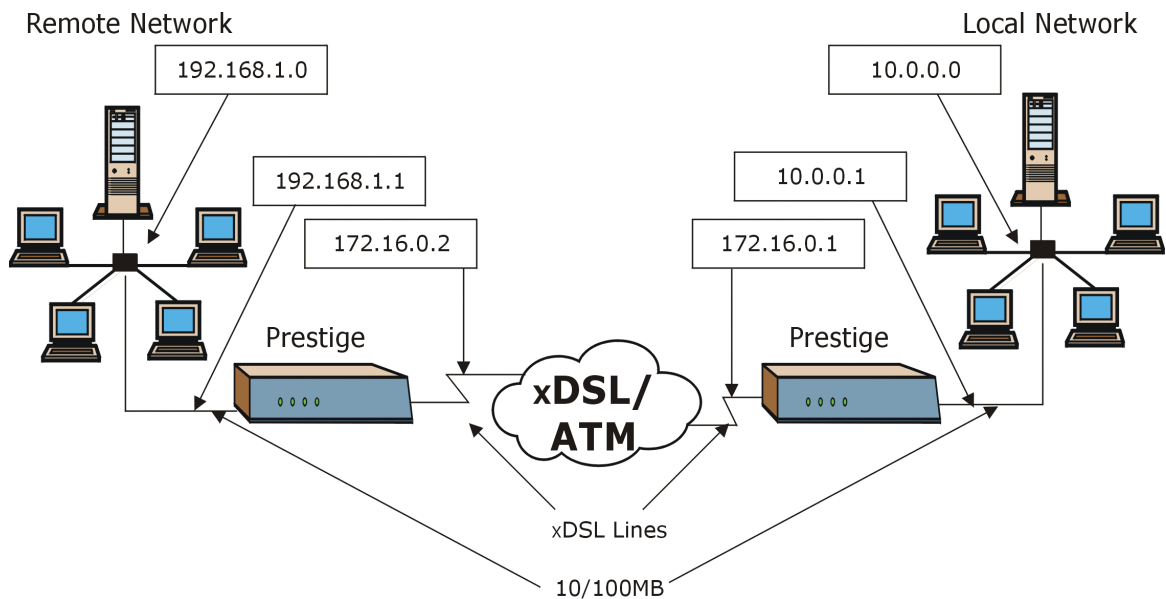


Figure 6-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure fields in **Menu 11.1 – Remote Node Profile**, as shown in the following table. For more details on the IP Option fields, refer to *Internet Access*.

Table 6-1 TCP/IP-Related Fields in Menu 11.1 — Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Route	Make sure IP is among the protocols in the Route field in Menu 11.1 – Remote Node Profile .	IP
Edit IP/Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display menu.	Yes

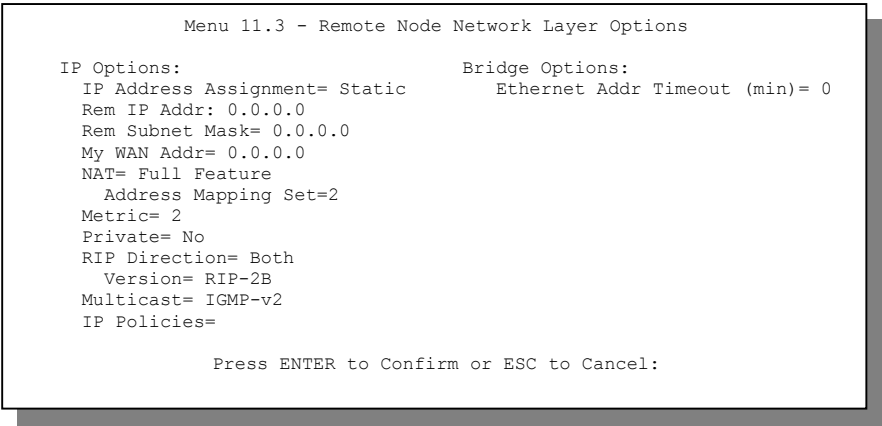


Figure 6-4 Remote Node Network Layer Options

The following table shows the fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 6-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic if the remote node is using a dynamically assigned IP address or Static if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (the first node); all other nodes are set to Static .	Static
Rem IP Addr	This is the IP address of the remote gateway. Type the remote Prestige's WAN IP address here (172.16.02 in the example <i>Figure 6-3</i> shown previously). If the remote Prestige's WAN IP address is 0.0.0.0, then type 192.168.1.1 (its LAN IP address) here.	0.0.0.0 (default)
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	0.0.0.0 (default)
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.	
NAT	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige.	Full Feature

FIELD	DESCRIPTION	EXAMPLE
(Network Address Translation)	Select SUA Only if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section 8.3.1). Select None to disable NAT.	
Address Mapping Set	When Full Feature is selected in the NAT field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the <i>NAT</i> chapter for details) and type that number here. When SUA Only is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the <i>NAT</i> chapter for details).	2
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	Yes
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are Both , In Only , Out Only or None .	Both
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are RIP-1 , RIP-2B or RIP-2M .	RIP-2B
Multicast	IGMP-v1 sets IGMP to version 1, IGMP-v2 sets IGMP to version 2 and None disables IGMP.	IGMP-v2
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

6.1.2 IP Static Route Setup

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to

network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the Prestige about the networks beyond the remote nodes.

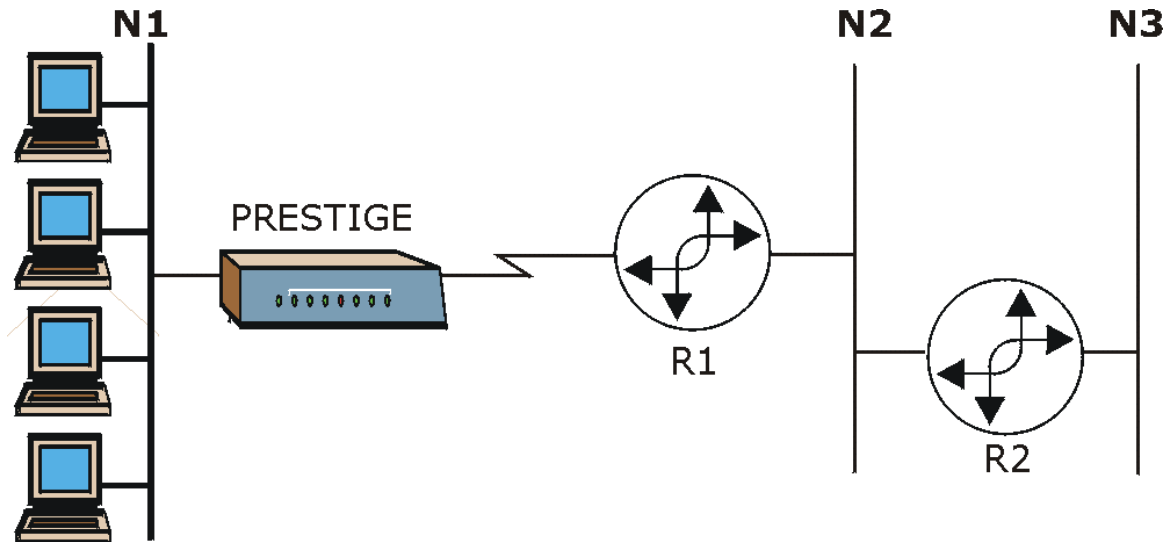


Figure 6-5 Sample Static Routing Topology

Configuration

Step 1. To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).


```
Menu 12 - Static Route Setup

1. IP Static Route
3. Bridge Static Route

Please enter selection:
```

Figure 6-6 Menu 12 — Static Route Setup

Step 2. From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

```
Menu 12.1 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter selection number:
```

Figure 6-7 Menu 12.1 — IP Static Route Setup

Step 3. Now, type the route number of a static route you want to configure.

```
Menu 12.1.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-8 Edit IP Static Route

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

Table 6-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and is not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 7

Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

7.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

7.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

- Step 1.** In menu 11.1, make sure the **Bridge** field is set to **Yes**.
- Step 2.** Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

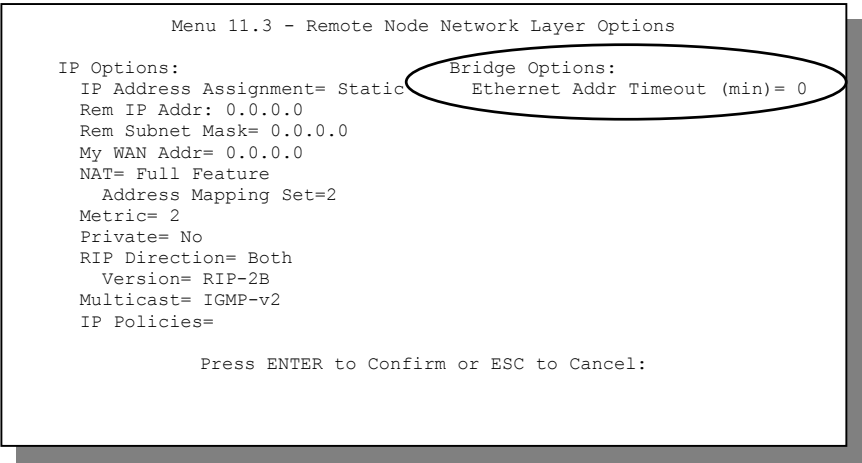


Figure 7-1 Menu 11.3 — Remote Node Bridging Options

Table 7-1 Remote Node Bridge Options

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to Yes .
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select Yes and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

7.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

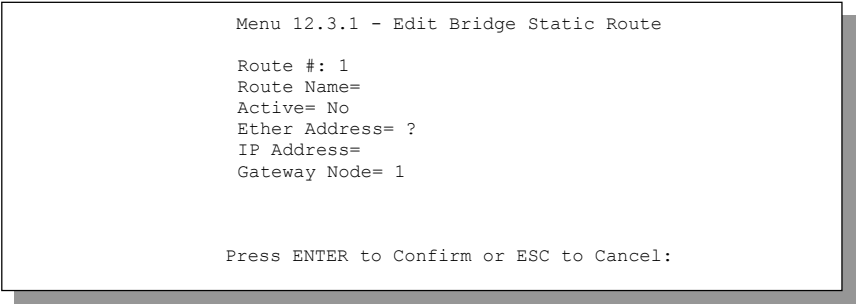


Figure 7-2 Menu 12.3.1 — Edit Bridge Static Route

The following table describes the **Edit Bridge Static Route** menu.

Table 7-2 Edit Bridge Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the route index number you typed in Menu 12.3 – Bridge Static Route Setup .
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (Yes) or not (No).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 8

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

8.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is travelling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 8-1 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 8-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

8.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

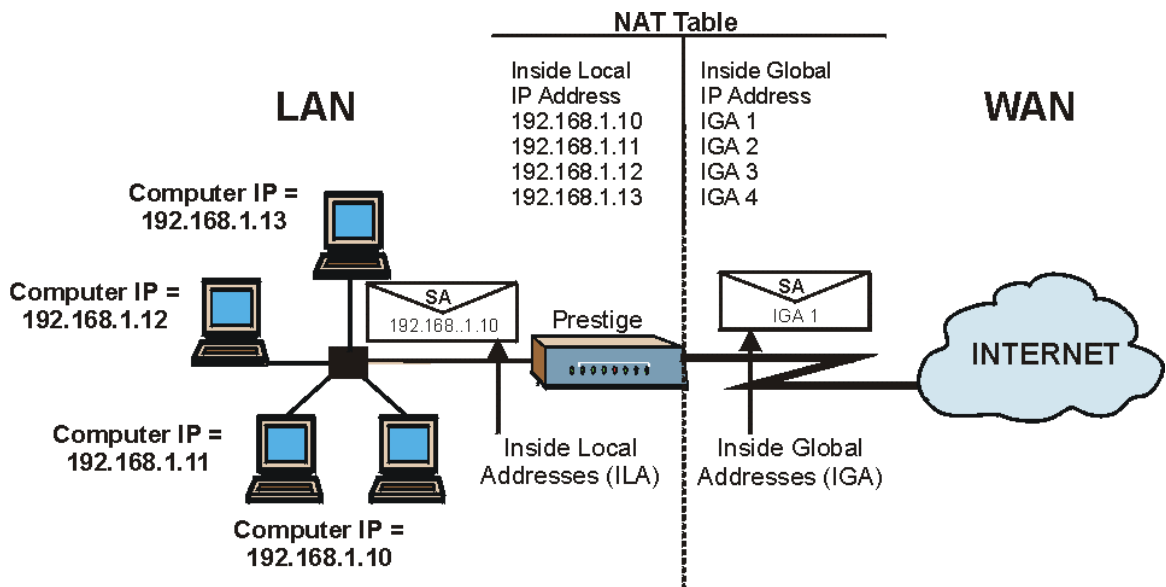


Figure 8-1 How NAT Works

8.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Prestige can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

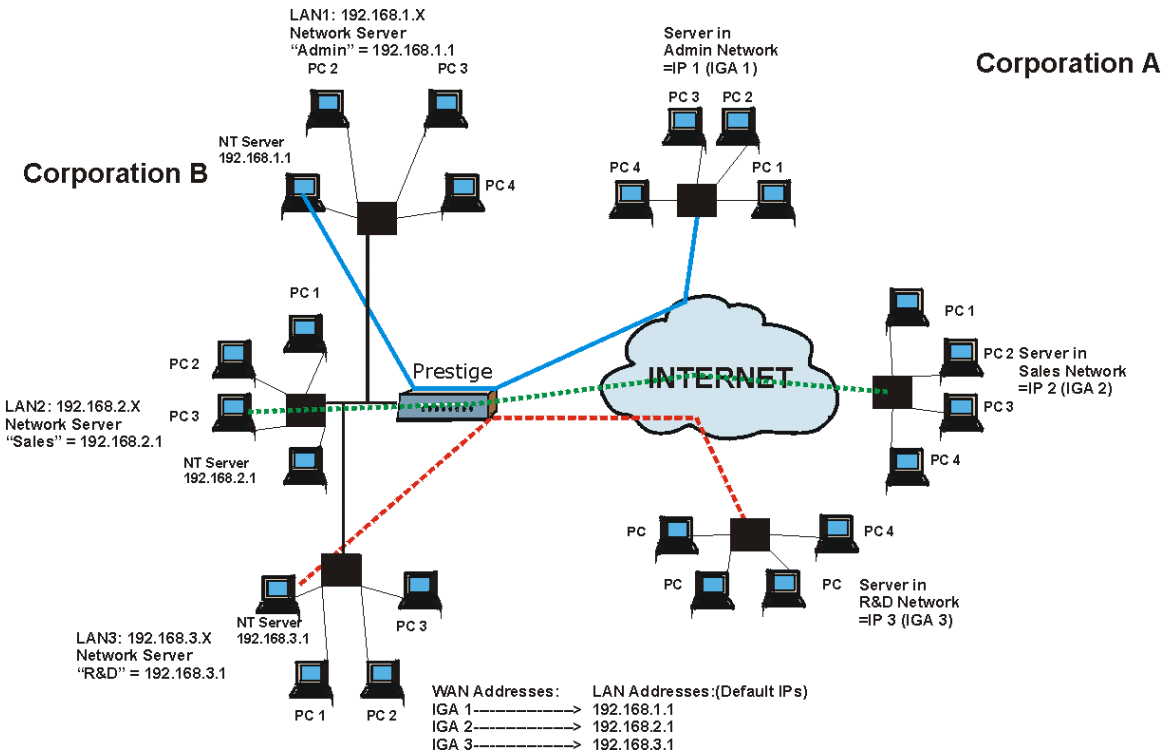


Figure 8-2 NAT Application With IP Alias

8.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. **One to One:** In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. **Many to One:** In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload:** In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.
5. **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do not change for One-to-One and Many-to-Many No Overload NAT mapping types.

The following table summarizes these types.

Table 8-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1↔ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1↔ IGA1 ILA2↔ IGA1 ...	M:1
Many-to-Many Overload	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA1 ILA4↔ IGA2 ...	M:M Ov
Many-to-Many No Overload	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA3 ...	M:M No OV
Server	Server 1 IP↔ IGA1 Server 2 IP↔ IGA1 Server 3 IP↔ IGA1	Server

8.2 Using NAT

In addition to setting up SUA/NAT, you must create a firewall rule to allow traffic from the WAN to be forwarded through the Prestige.

8.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section 8.3.1 for a detailed description of the NAT set for SUA.

The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 8-2*.

1. **Choose SUA Only if you have just one public WAN IP address for your Prestige.**
2. **Choose Full Feature if you have multiple public WAN IP addresses for your Prestige.**

8.2.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

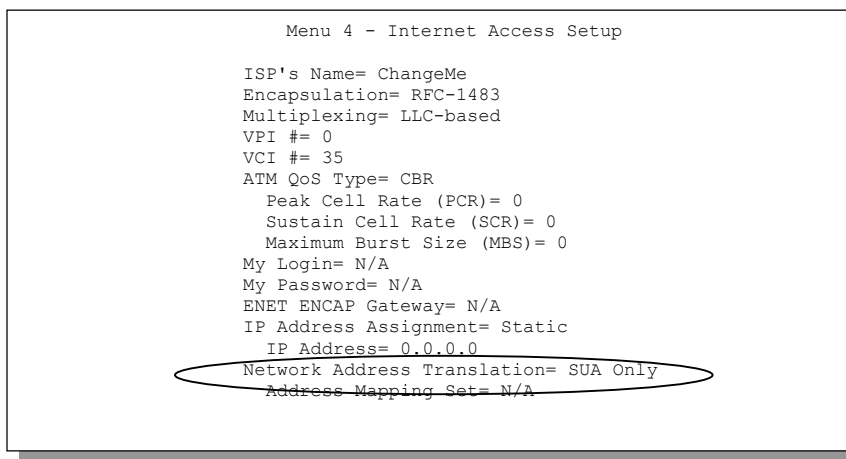


Figure 8-3 Menu 4 — Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

- Step 1.** Enter 11 from the main menu.
- Step 2.** Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

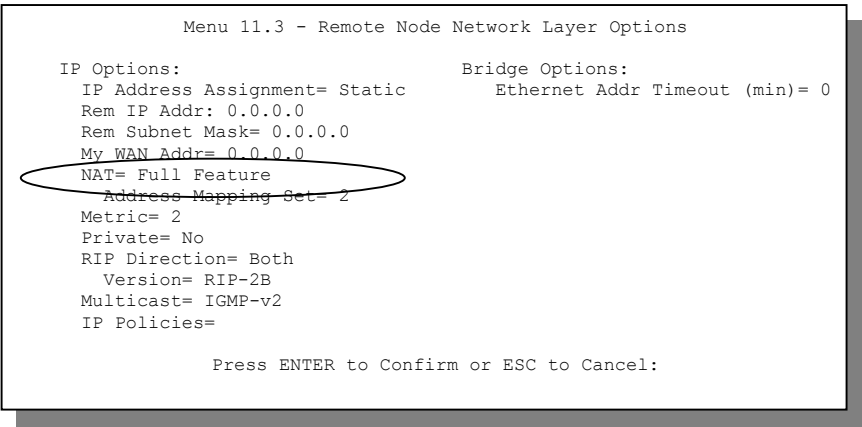


Figure 8-4 Menu 11.3 — Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 8-3 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	OPTIONS
NAT (Network Address Translation)	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the Address Mapping Set field (menu 15.1 - see section 8.3.1).	Full Feature
	Select None to disable NAT.	None
	When you select SUA Only , the SMT uses Address Mapping Set 255 (menu 15.1 - see section 8.3.1). Choose SUA Only if you have just one public WAN IP address for your Prestige.	SUA Only

8.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in Table 8-2. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige); a server rule must be set up inside the NAT Address Mapping set. Please see *section 8.4* for

further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

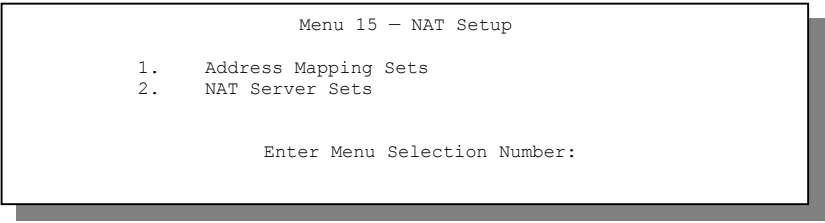


Figure 8-5 Menu 15 — NAT Setup

8.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

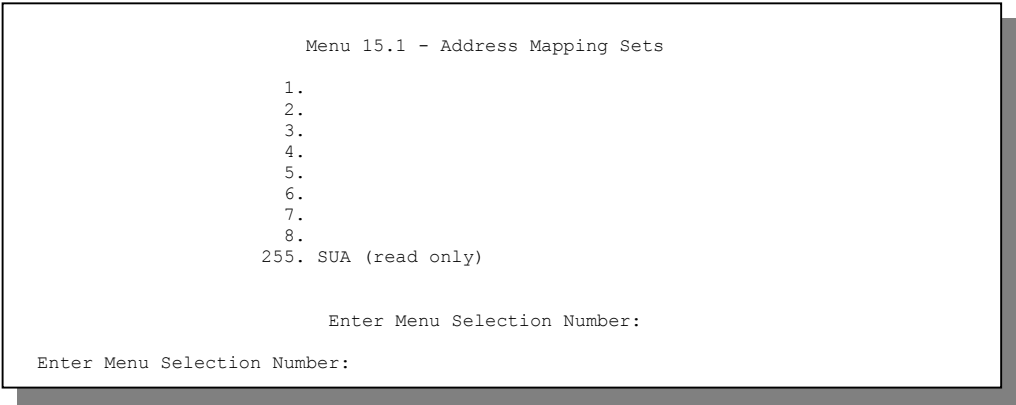


Figure 8-6 Menu 15.1 — Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 8.2.1*). The fields in this menu cannot be changed.

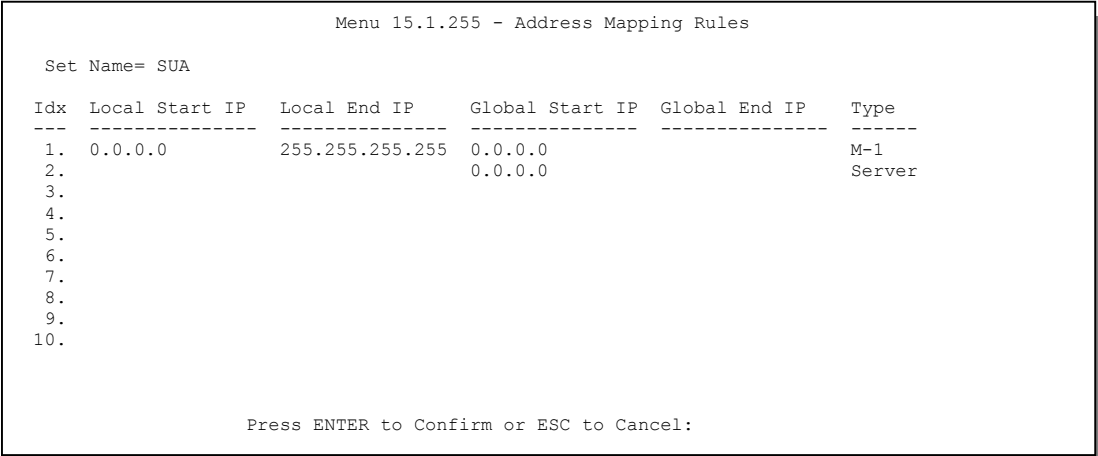


Figure 8-7 Menu 15.1.255 — SUA Address Mapping Rules

The following table explains the fields in this screen.

Menu 15.1.255 is read-only.

Table 8-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA (default)
Idx	This is the index or rule number.	1
Local Start IP Local End IP	Local Start IP is the starting local IP address (ILA) (see Figure 8-1). Local End IP is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP .	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	

FIELD	DESCRIPTION	EXAMPLE
Type	These are the mapping types discussed above (see <i>Table 8-2</i>). Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now let’s look at option 1 in menu 15.1. Enter 1 to bring up this menu. We’ll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

If the Set Name field is left blank, the entire set will be deleted.

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit Select Rule=

Press ENTER to Confirm or ESC to Cancel:

Figure 8-8 Menu 15.1.1 — First Set

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are

ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 8-5 Fields in Menu 15.1.1

FIELD	DESCRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is Edit . Edit means you want to edit a selected rule (see following field). Insert Before means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. Delete means to delete the selected rule and then all the rules after the selected one will be advanced one rule. None disables the Select Rule item.	Edit
Select Rule	When you choose Edit , Insert Before or Delete in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

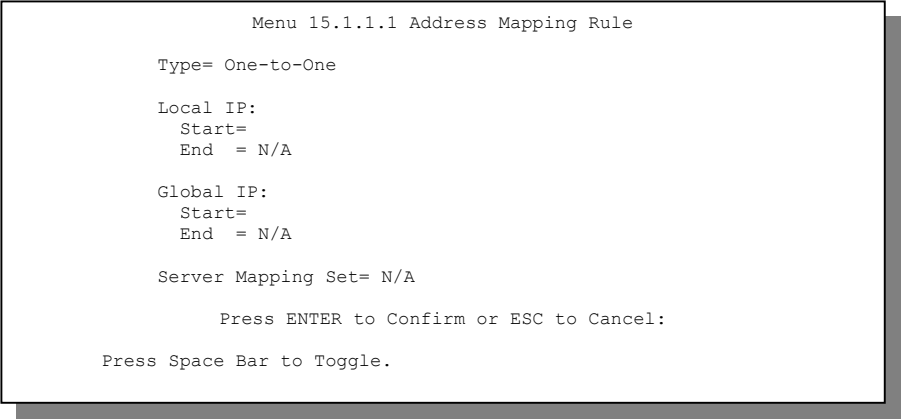


Figure 8-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

Table 8-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Table 8-2. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 8.5.3</i> for an example.	One-to-One
Local IP	Only local IP fields are N/A for server; Global IP fields MUST be set for Server .	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is N/A for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global IP Start . Note that Global IP Start can be set to 0.0.0.0 only if the types are Many-to-One or Server .	0.0.0.0
End	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server types.	N/A
Server Mapping	Only available when Type is set to Server . Type a number from 1 to 10 to choose a server set from menu 15.2.	

FIELD	DESCRIPTION	EXAMPLE
Set		
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.		

8.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 8-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79

SERVICES	PORT NUMBER
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

8.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

- Step 1.** Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- Step 2.** Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

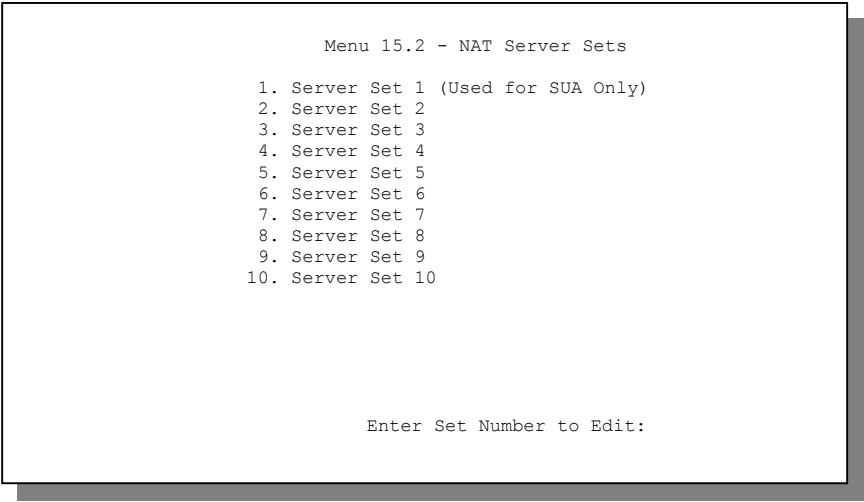


Figure 8-10 Menu 15.2 — NAT Server Setup

- Step 3.** Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

Menu 15.2.1 - NAT Server Setup (Used for SUA Only)

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Figure 8-11 Menu 15.2.1 — NAT Server Setup

- Step 4.** Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- Step 5.** Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- Step 6.** Press [ENTER] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

The NAT network appears as
a single host on the Internet

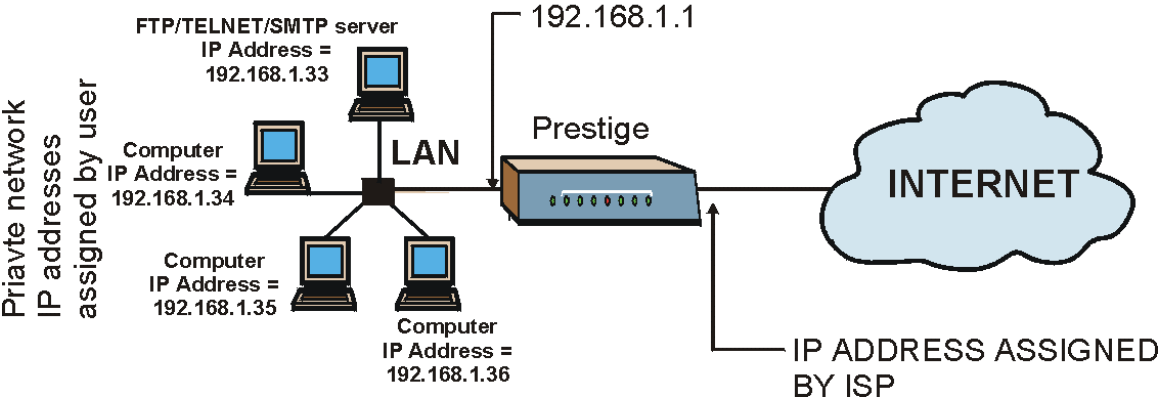


Figure 8-12 Multiple Servers Behind NAT Example

8.5 General NAT Examples

8.5.1 Example 1 Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

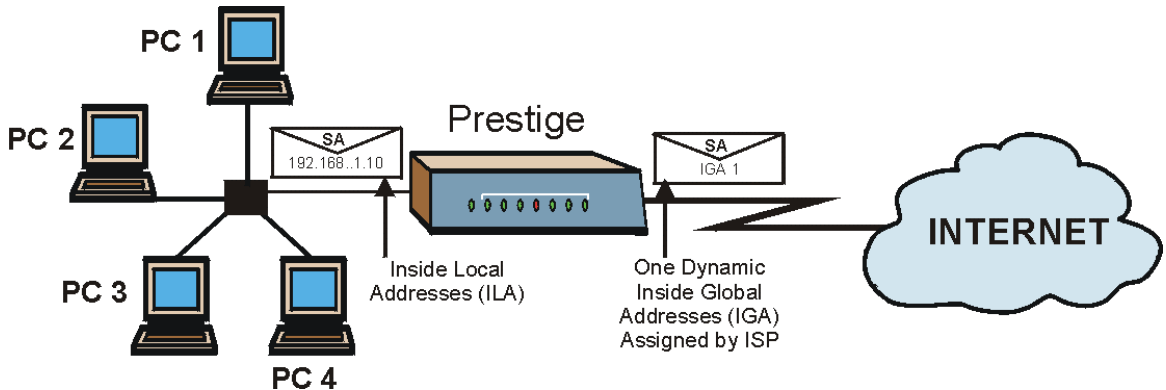


Figure 8-13 NAT Example 1

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= RFC-1483
Multiplexing= LLC-based
VPI #= 1
VCI #= 1
ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 5500
    Sustained Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
IP Address= 0.0.0.0
Network Address Translation= SUA Only
Address Mapping Set=
  
```

Figure 8-14 Menu 4 — Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 8.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

8.5.2 Example 2: Internet Access with an Inside Server

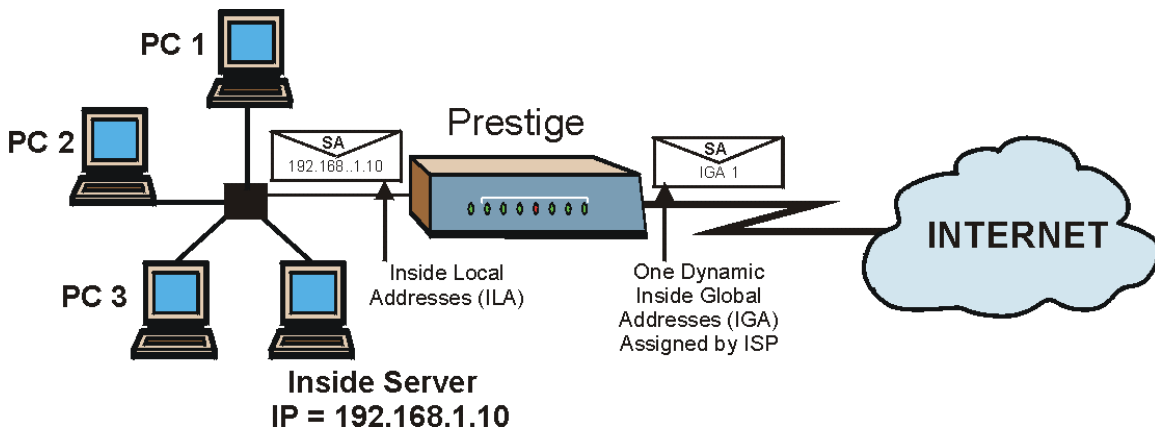


Figure 8-15 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

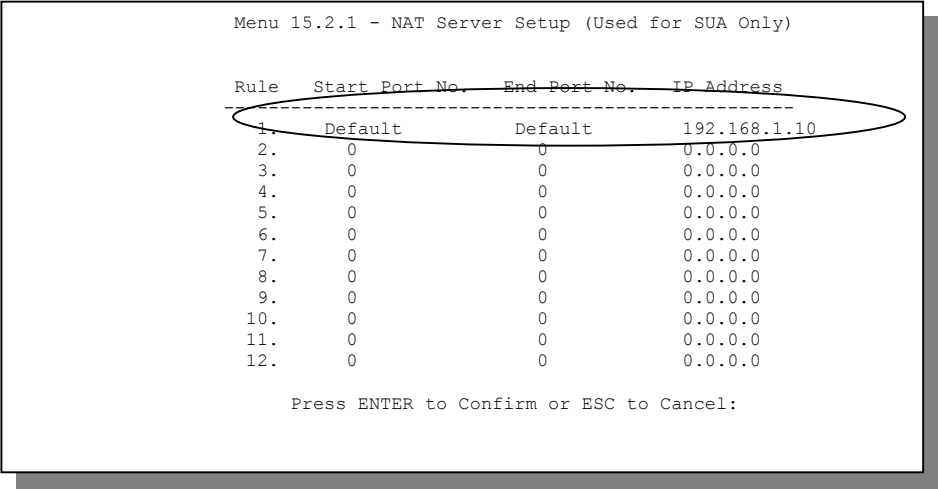


Figure 8-16 Menu 15.2.1 — Specifying an Inside Server

8.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP servers. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

- Rule 1.** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 2.** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- Rule 4.** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

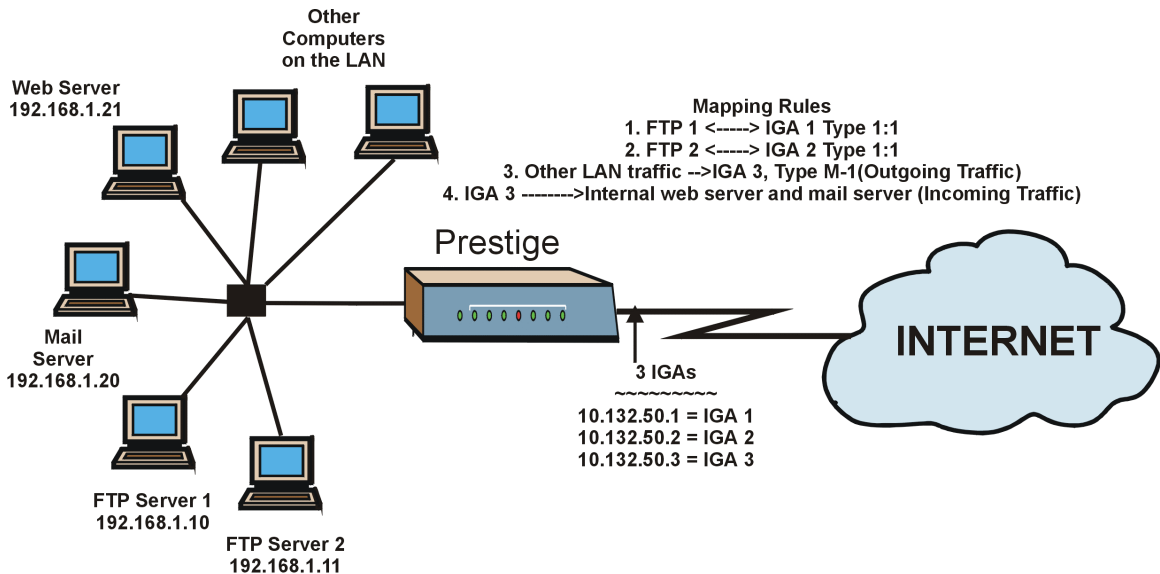


Figure 8-17 NAT Example 3

- Step 1.** In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 8-18.
- Step 2.** Then enter 15 from the main menu.
- Step 3.** Enter 1 to configure the Address Mapping Sets.
- Step 4.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- Step 5.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 8-19*).
- Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.
- Step 7.** When finished, menu 15.1.1 should look like as shown in *Figure 8-20*.

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:                                Bridge Options:
IP Address Assignment= Static              Ethernet Addr Timeout (min)= 0
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
NAT= Full Feature
Address Mapping Set= 2
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies=

Press ENTER to Confirm or ESC to Cancel:
```

Figure 8-18 Example 3: Menu 11.3

The following figure shows how to configure the first rule.

```
Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
Start= 192.168.1.10
End = N/A
Global IP:
Start= 10.132.50.1
End = N/A
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-19 Example 3: Menu 15.1.1.1

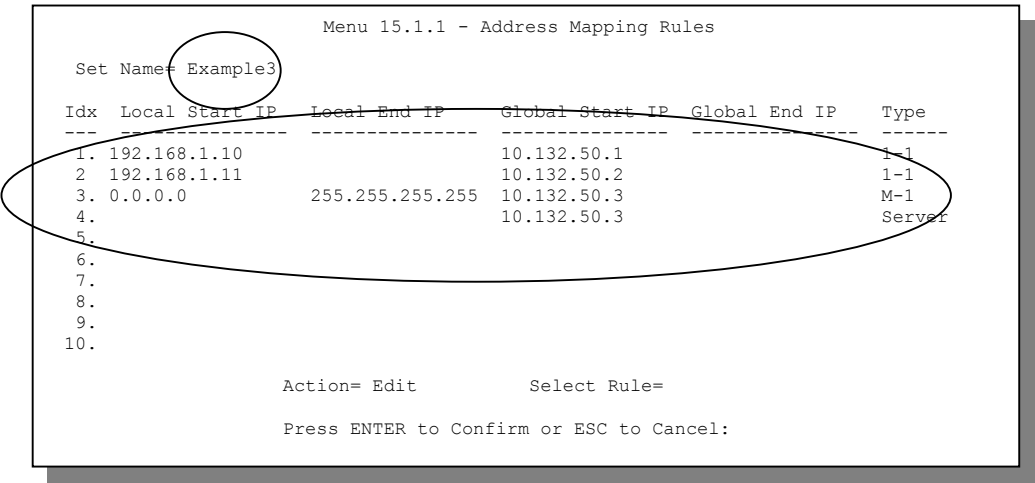


Figure 8-20 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

- Step 8.** Enter 15 from the main menu.
- Step 9.** Enter 2 in **Menu 15 - NAT Setup**.
- Step 10.** Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

Menu 15.2.1 - NAT Server Setup (Used for SUA Only)

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Example 3: Menu 15.2.1

8.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

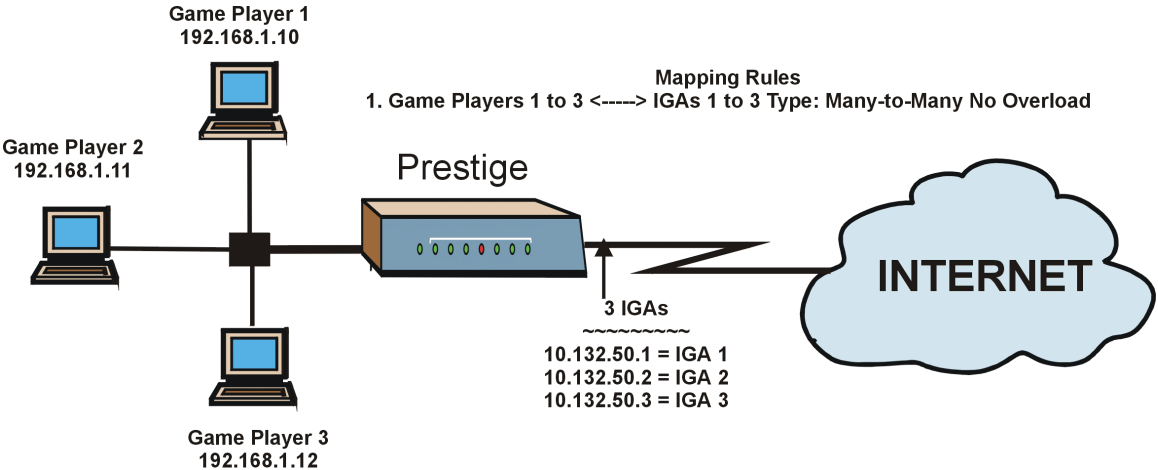


Figure 8-21 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows.

```
Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figure 8-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

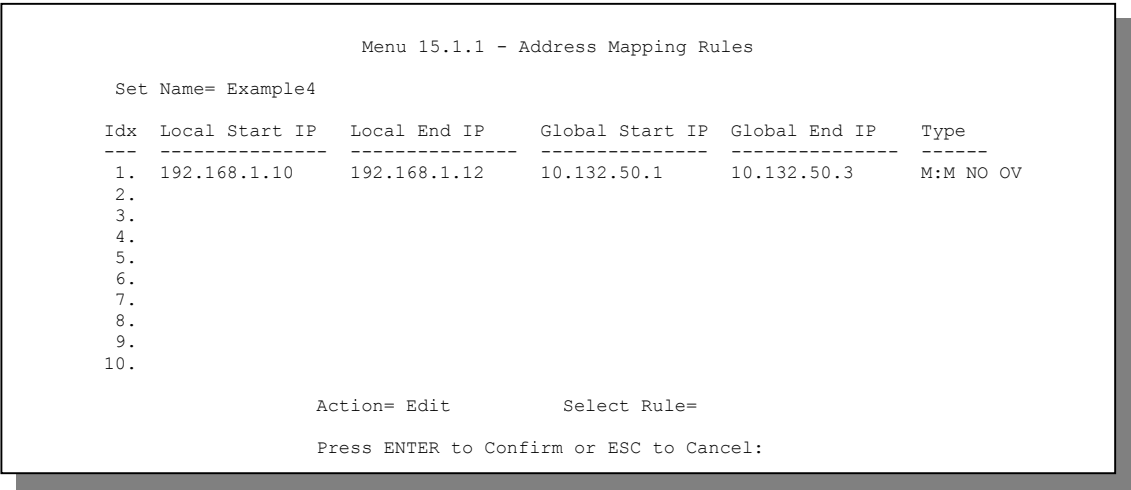


Figure 8-23 Example 4: Menu 15.1.1 — Address Mapping Rules

Part III:

Firewall and Content Filters

Part III introduces firewalls in general and the Prestige firewall. It also explains customized services and logs and gives example firewall rules and an overview of content filtering.

Chapter 9

Firewalls

This chapter gives some background information on firewalls and explains how to get started with the Prestige firewall.

9.1 What Is a Firewall?

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term “firewall” is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

9.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

9.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

9.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
- ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

9.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See *section 9.5* for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

9.3 Introduction to ZyXEL's Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The Prestige also has packet filtering capabilities.

The Prestige is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Prestige has one ADSL port and one Ethernet LAN port, which physically separate the network into two areas.

- ❑ The ADSL port connects to the Internet.
- ❑ The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

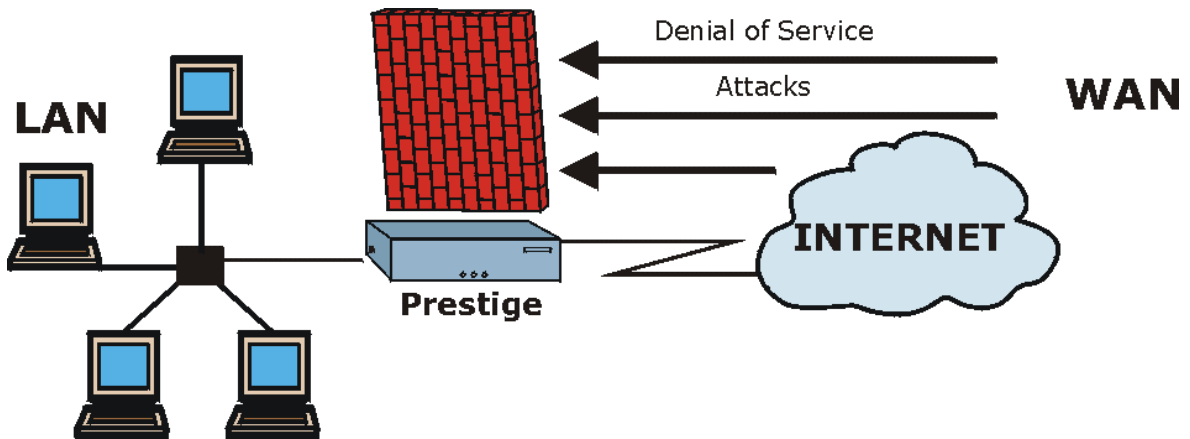


Figure 9-1 Prestige Firewall Application

9.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Prestige is pre-configured to automatically detect and thwart all known DoS attacks.

9.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the “TCP port” or “UDP port” identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server “listens” on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

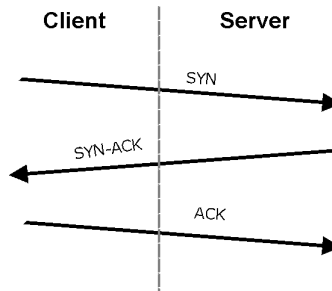
Table 9-1 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

9.4.2 Types of DoS Attacks

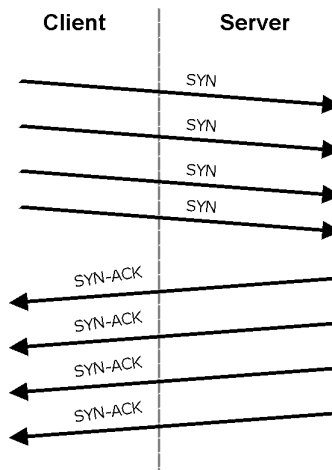
There are four types of DoS attacks:

- 1. Those that exploit bugs in a TCP/IP implementation.
 - 2. Those that exploit weaknesses in the TCP/IP specification.
 - 3. Brute-force attacks that flood a network with useless data.
 - 4. IP Spoofing.
- 1. **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
 - 1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
 - 1-b Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
 - 2. Weaknesses in the TCP/IP specification leave it open to **"SYN Flood"** and **"LAND"** attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

**Figure 9-2 Three-Way Handshake**

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

2-a **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

**Figure 9-3 SYN Flood**

- 2-b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.
3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

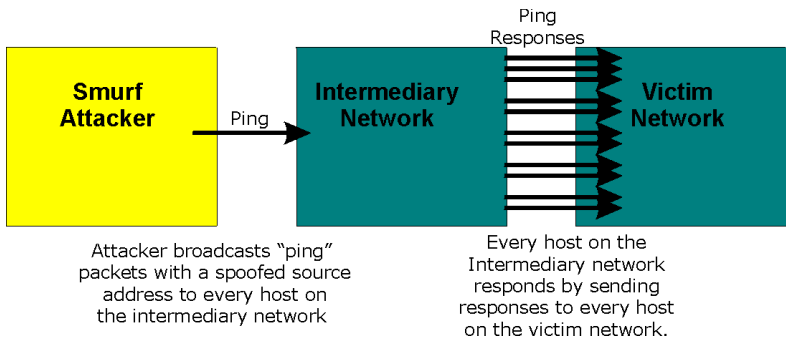


Figure 9-4 Smurf Attack

❑ ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 9-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

❑ Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 9-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 9-4 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VERFY	

❑ Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The Prestige blocks all IP Spoofing attempts.

9.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The Prestige uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the Prestige’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- ❑ Allows all sessions originating from the LAN (local network) to the WAN (Internet).

- ❑ Denies all sessions originating from the WAN to the LAN.

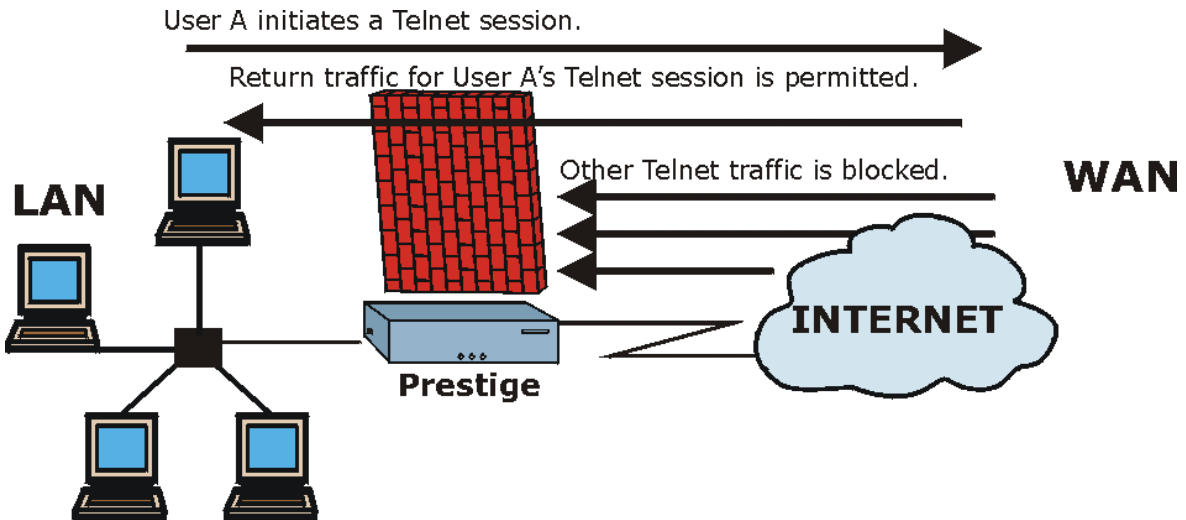


Figure 9-5 Stateful Inspection

The previous figure shows the Prestige's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

9.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see *Figure 12-3*) determines the action for this packet.

4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

9.5.2 Stateful Inspection and the Prestige

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.
- iii. Allow access to a Web server to everyone but competitors.
- iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the Prestige itself (as with the "virtual connections" created for UDP and ICMP).

9.5.3 TCP Security

The Prestige uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the Prestige receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

9.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the Prestige is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too

little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

9.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the Prestige inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

9.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or web configurator.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

9.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

1. Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
2. DSL or cable modem connections are “always-on” connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
3. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
4. Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
5. Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small “key” icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
6. Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
7. Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
8. Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
9. If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.
10. If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
11. Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

9.7 Packet Filtering Vs Firewall

Below are some comparisons between the Prestige’s filtering and firewall functions.

9.7.1 Packet Filtering:

- ❑ The router filters packets as they pass through the router's interface according to the filter rules you designed.
- ❑ Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- ❑ Packet filtering only checks the header portion of an IP packet.

When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

9.7.2 Firewall

- ❑ The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- ❑ The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- ❑ The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- ❑ The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 10

Introducing the Prestige Firewall

This chapter shows you how to get started with the Prestige firewall.

10.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

10.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

10.3 Using Prestige SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

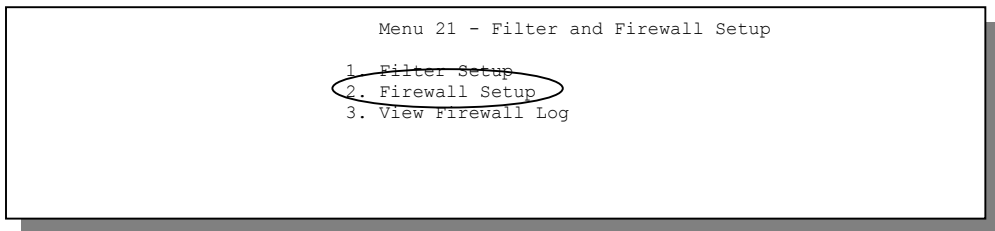


Figure 10-1 Menu 21 — Filter and Firewall Setup

10.3.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

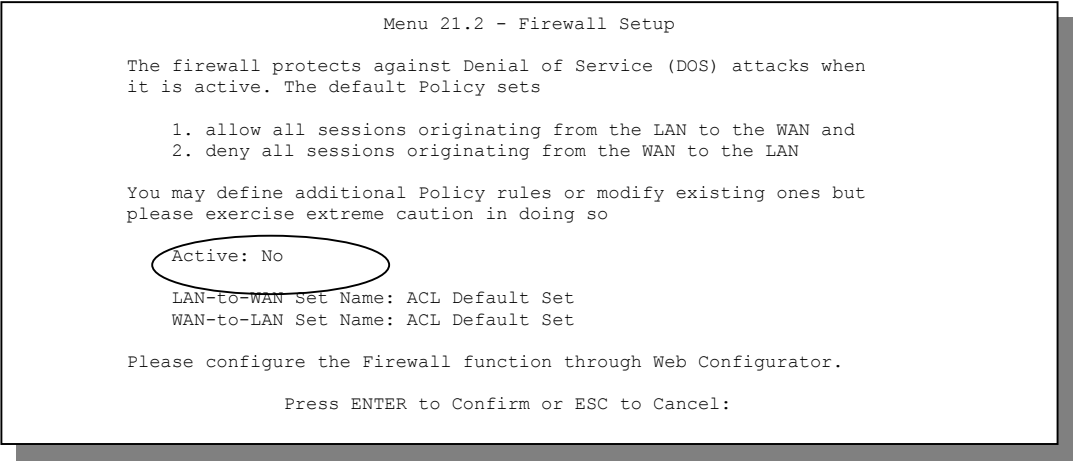


Figure 10-2 Menu 21.2 — Firewall Setup

Configure the firewall rules using the web configurator or CLI commands.

10.3.2 Viewing the Firewall Log

In menu 21, enter 3 to view the firewall log. An example of a firewall log is shown next.

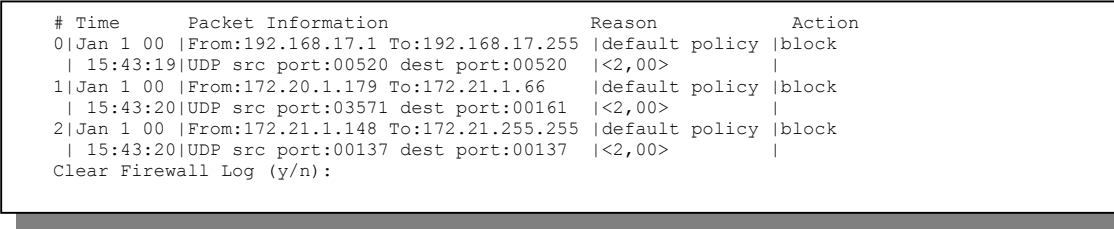


Figure 10-3 Example Firewall Log

An “End of Log” message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

Table 10-1 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the Prestige was reset.	mm:dd:yy e.g., Jan 1 00 ----- hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses ----- Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, did not match or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule. This is a log for a DoS attack.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol. ----- attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked or forwarded. None means that no action is dictated by this rule.	block, forward or none
After viewing the firewall log, ENTER “y” to clear the log or “n” to retain it. With either option you will be returned to Menu 21- Filter and Firewall Setup .		

Chapter 11

Using the Prestige Web Configurator

This chapter shows you how to configure your firewall with the web configurator.

11.1 Web Configurator Login and Main Menu Screens

Use the Prestige web configurator, to configure your firewall. To get started, follow the steps shown next.

Step 1. Launch your web browser and enter 192.168.1.1 as the URL.

Step 2. Enter “admin” as the user name and "1234" (default) as the password and click **Login**.

Step 3. The **Site Map** screen displays.

Use the help icon (located in the upper right portion of most screens) for explanations of fields and choices.

If you forget your password, refer to the *Resetting the Prestige* section to see how to reset the default configuration file.

11.2 Enabling the Firewall

Click **Advanced Setup**, **Firewall**, and then **Config** to display the following screen. Click the **Firewall Enabled** check box to enable (or activate) the firewall.

The screenshot shows the ZyXEL web configuration interface. On the left is a navigation menu with the following items: Wizard Setup, Advanced Setup (selected), Password, LAN, NAT, Dynamic DNS, Time Zone, Content Filter, Firewall (sub-selected), VPN, Remote Management, Maintenance, and Logout. The main content area is titled "Firewall - Configuration - Config". It features a checkbox labeled "Firewall Enabled" which is currently unchecked. Below this, a text block states: "The firewall protects against Denial of Service (DOS) attacks when it is active. The default Policy sets" followed by a numbered list: "1. allow all sessions originating from the Local Network to the Internet and" and "2. deny all sessions originating from the Internet to the Local Network". Another text block follows: "You may define additional Policy rules or modify existing ones but please exercise extreme caution in doing so" followed by a numbered list: "1. Local Network to Internet Set" and "2. Internet to Local Network Set". A caution note at the bottom reads: "CAUTION: If Firewall Enabled is not checked, all the existing firewall security policies and firewall functions will be disabled." At the bottom right of the main area are three buttons: "Back", "Apply", and "Reset".

Figure 11-1 Enabling the Firewall

11.3 E-mail

The E-mail screen allows you to specify your mail server, where e-mail alerts should be sent as well as when and how often they should be sent.

11.3.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen (*Figure 11-4* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Rule Config** screen (see *Figure 12-4*). When an event generates an alert, a message is immediately sent to an e-mail account specified by

you. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Log Timer** fields in the **E-mail** screen (following screen).

11.3.2 Logs

A log is a detailed record that you create for packets that either match a rule, don't match a rule or both when you are creating/editing a firewall rule (see *Figure 12-4*). You can also choose not to create a log for a rule in this screen. An attack automatically generates a log.

Click **Advanced Setup**, **Firewall**, and then **E-mail** to bring up the following screen.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

[SITE MAP](#) [HELP](#)

Wizard Setup

Advanced Setup

- Password
- LAN
- NAT
- Dynamic DNS
- Time Zone
- Content Filter
- Firewall
- VPN
- Remote Management

Maintenance

Logout

Firewall - Email

Address Info

Mail Server:

Subject:

E-mail Alerts To: (Email)

Return Address: (Email)

Log Timer

Log Schedule:

Day for Sending Alerts:

Time for Sending Alerts: (hour) : (minute)

Figure 11-2 E-mail Screen

The following table describes the fields in this screen.

Table 11-1 E-mail

FIELD	DESCRIPTION	OPTIONS
Address Info Mail Server	Enter the IP address of your mail server in dotted decimal notation. Your Internet Service Provider (ISP) should be able to provide this information. If this field is left blank, log and alert messages will not be sent via e-mail.	
Mail Subject	Enter a subject that you want to appear in the subject field of your e-mail here (see <i>Figure 11-3</i>). If you leave this field blank then the default “Firewall Alert From Prestige” displays as your e-mail subject.	
E-mail Alerts To	Enter the e-mail address (username@mydomain.com) of whoever is responsible for maintaining the firewall, e.g., your system administrator. If this field is left blank, alert messages will not be sent via e-mail.	
Return address	Enter an e-mail address to identify the Prestige as the sender of the e-mail messages i.e., a “return-to-sender” address for backup purposes.	
Log Timer Log Schedule	This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, hourly, only when the log is full or none. If the Weekly or the Daily option is selected, specify a time of day when the e-mail should be sent. If the Weekly option is selected, then also specify which day of the week the e-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None , no log messages are e-mailed.	When Log is Full Hourly Daily Weekly None
Day for Sending Alerts	Click which day of the week you want to send the alert from the drop down list box.	Sunday through Saturday
Time for Sending Alerts	Click the up or down arrows to the right of the list box to choose a time to send the alerts.	
Click Back to return to the previous screen. Click Apply to save your customized settings and exit this screen. Click Reset to return to the previous configuration. Use the Help icon to find field descriptions.		

11.3.3 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear. Please see the *Support Notes* on the included disk for information on other types of error messages.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??" are described in the following table.

Table 11-2 SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

11.3.4 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

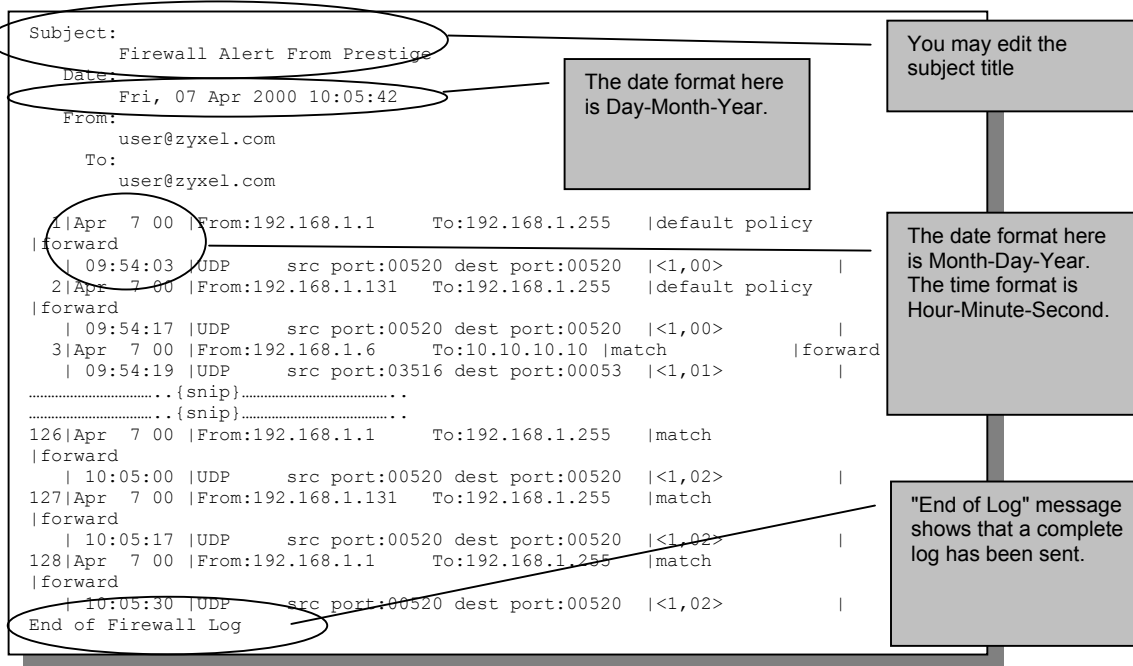


Figure 11-3 E-mail Log

11.4 Attack Alert

Attack alerts are the first defense against DoS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the Prestige uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

11.4.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.

2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

11.4.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TCP three-way handshake has not yet been completed (see *Figure 9-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

The Prestige measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the Prestige starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Time** timeout is 0 (the default), then the Prestige deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- 2. If the **Blocking Time** timeout is greater than 0, then the Prestige blocks all new connection requests to the host giving the server time to handle the present connections. The Prestige continues to block all new connection requests until the **Blocking Time** expires.

The Prestige also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click **Advanced Setup**, **Firewall**, and **Alert** to bring up the next screen.

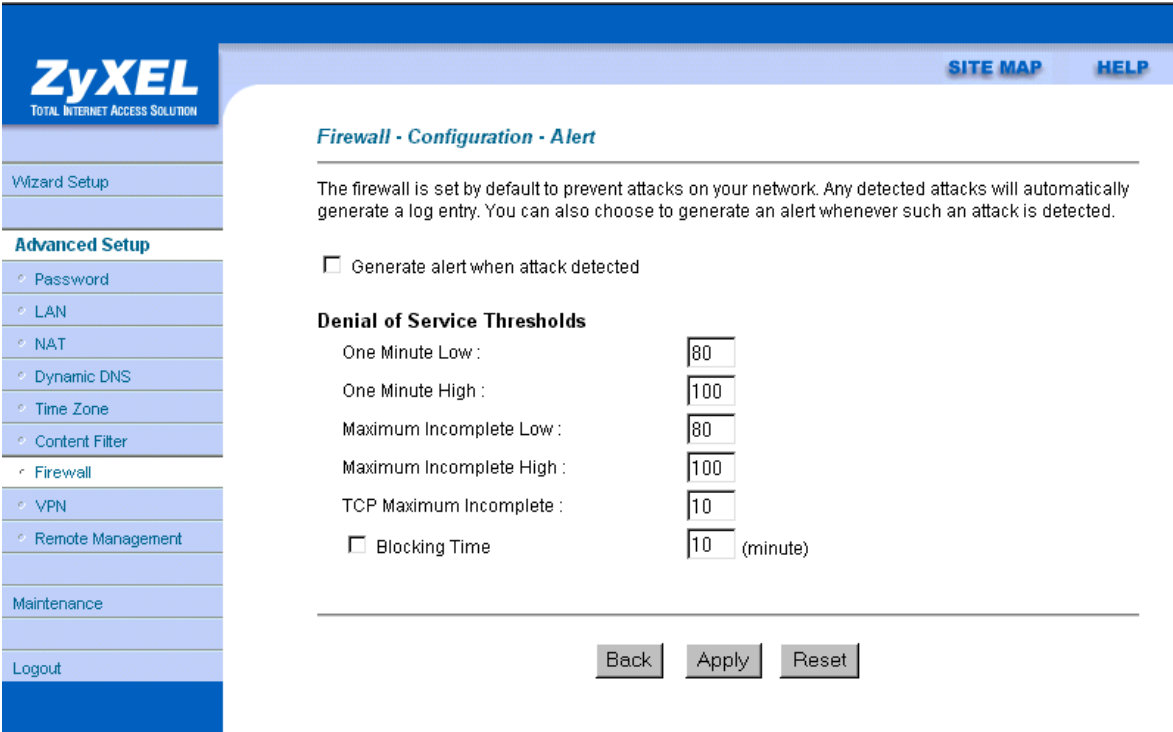


Figure 11-4 Attack Alert

The following table describes the fields in this screen.

Table 11-3 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the <i>Logs Chapter</i> for more information on logs and alerts.	
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the Prestige to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Prestige	100 half-open sessions per minute. The above values causes the Prestige to start deleting half-open sessions when the number of existing

Table 11-3 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
	deletes half-open sessions as required to accommodate new connection requests. Do not set Maximum Incomplete High to lower than the current Maximum Incomplete Low number.	half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.
Blocking Time	When TCP Maximum Incomplete is reached you can choose if the next session should be allowed or blocked. If you check Blocking Time any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	10 minutes (default)
(min)	Enter the length of Blocking Time in minutes.	0
Click Back to return to the previous screen. Click Apply to save your customized settings and exit this screen. Click Reset to return to the previous configuration. Use the Help icon to view field descriptions.		

Chapter 12

Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules.

12.1 Rules Overview

Firewall rules are subdivided into “Local Network” and “Internet”. By default, the Prestige’s stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

You might inadvertently introduce security risks to the firewall and to the protected network, if you try to configure rules without a good understanding of how rules work. Make sure you test your rules after you configure them.

For example, you may create rules to:

- ◆ Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- ◆ Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- ◆ Allow everyone except your competitors to access a Web server.
- ◆ Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing network traffic’s Source IP address, Destination IP address, IP protocol type to rules set by the administrator. Your customized rules take precedence, and may override the Prestige’s default rules.

12.2 Rule Logic Overview

Study these points carefully before configuring rules.

12.2.1 Rule Checklist

1. State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
2. Is the intent of the rule to forward or block traffic?

3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.2.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the web configurator.

12.2.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

“Block” means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 12.5* for more information on predefined services.

Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

12.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

12.3.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure Policy -> LAN to WAN -> Rules, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

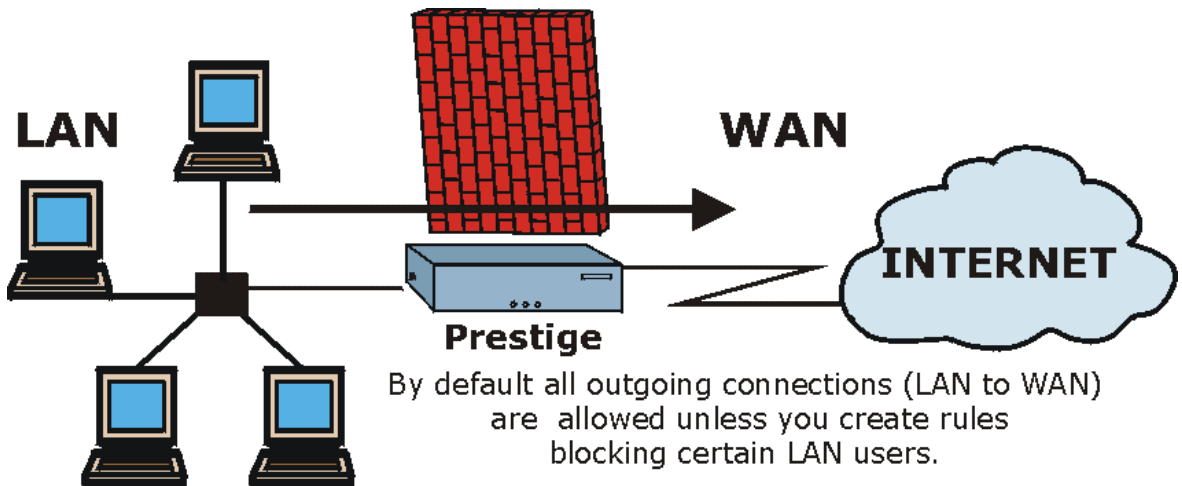


Figure 12-1 LAN to WAN Traffic

12.3.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

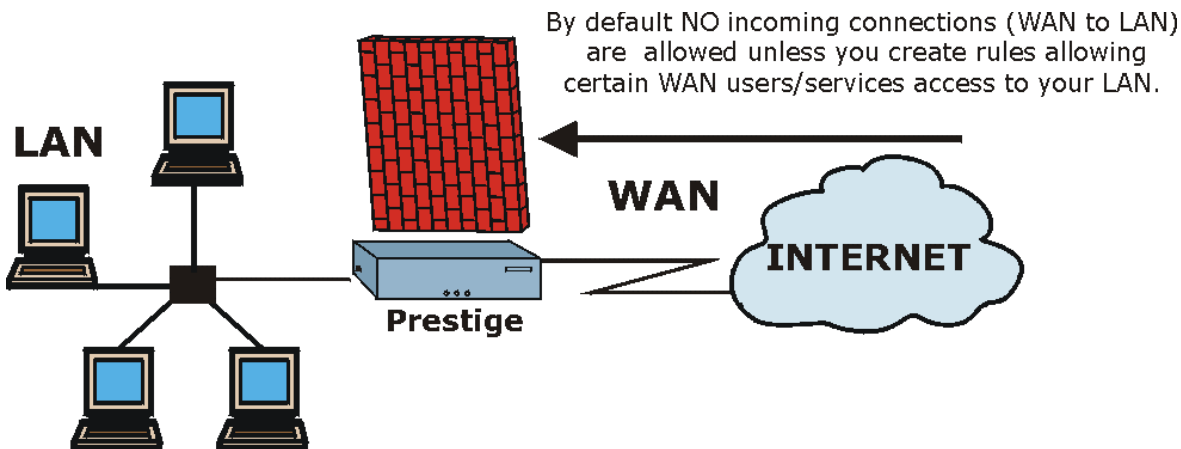


Figure 12-2 WAN to LAN Traffic

12.4 Rule Summary

The fields in the Rule Summary screens are the same for Local Network and Internet, so the discussion below refers to both.

Click on **Firewall**, then **Local Network** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

Wizard Setup

Advanced Setup

• Password

• LAN

• NAT

• Dynamic DNS

• Time Zone

• Content Filter

• Firewall

• VPN

• Remote Management

Maintenance

Logout

Firewall - LAN to WAN - Rule Summary

The default action for packets not matching following rules:

Forward

☒ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	<div></div>	<div></div>	<div></div>		
2	<div></div>	<div></div>	<div></div>		
3	<div></div>	<div></div>	<div></div>		
4	<div></div>	<div></div>	<div></div>		
5	<div></div>	<div></div>	<div></div>		
6	<div></div>	<div></div>	<div></div>		
7	<div></div>	<div></div>	<div></div>		
8	<div></div>	<div></div>	<div></div>		
9	<div></div>	<div></div>	<div></div>		
10	<div></div>	<div></div>	<div></div>		

Rules Reorder: Move rule number

1

 to rule number

1

Move

Back

Apply

Reset

Figure 12-3 Firewall Rules Summary — First Screen

The following table describes the fields in this screen.

Table 12-1 Firewall Rules Summary — First Screen

FIELD	DESCRIPTION	OPTIONS
The default action for packets not matching following rules	Should packets that do not match the following rules be blocked or forwarded? Make your choice from the drop down list box. Note that “block” means the firewall silently discards the packet.	Block Forward
Default Permit Log	Click this check box to log all matched rules in the ACL	

Table 12-1 Firewall Rules Summary — First Screen

FIELD	DESCRIPTION	OPTIONS
	default set.	
The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.		
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The Move field below allows you to reorder your rules. Click a rule's number to edit the rule.	
Source IP	This is the source address of the packet.	
Destination IP	This is the destination address of the packet.	
Service	This is the service to which the rule applies. See <i>Table 12-2</i> for more information.	
Action	This is the specified action for that rule. Note that Block means the firewall silently discards the packet.	Block Forward
Move Rule	You may reorder your rules using this function. Select by clicking on the rule you want to move. The ordering of your rules is important as rules are applied in turn.	
To Rule Number	Select the number you want to move the rule to.	
Move	Click Move to move the rule.	
Click Back to return to the previous screen. Click Apply to save your customized settings and exit this screen. Click Reset to return to the previous configuration. Click the Help icon for field descriptions.		

12.5 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see *Figure 12-4*) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 12-2 Predefined Services

SERVICE	DESCRIPTION
AIM(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20,21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.

Table 12-2 Predefined Services

SERVICE	DESCRIPTION
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.

Table 12-2 Predefined Services

SERVICE	DESCRIPTION
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

12.5.1 Creating/Editing Firewall Rules

To create a new rule, click a number (**No.**) in the last screen shown to display the following screen.

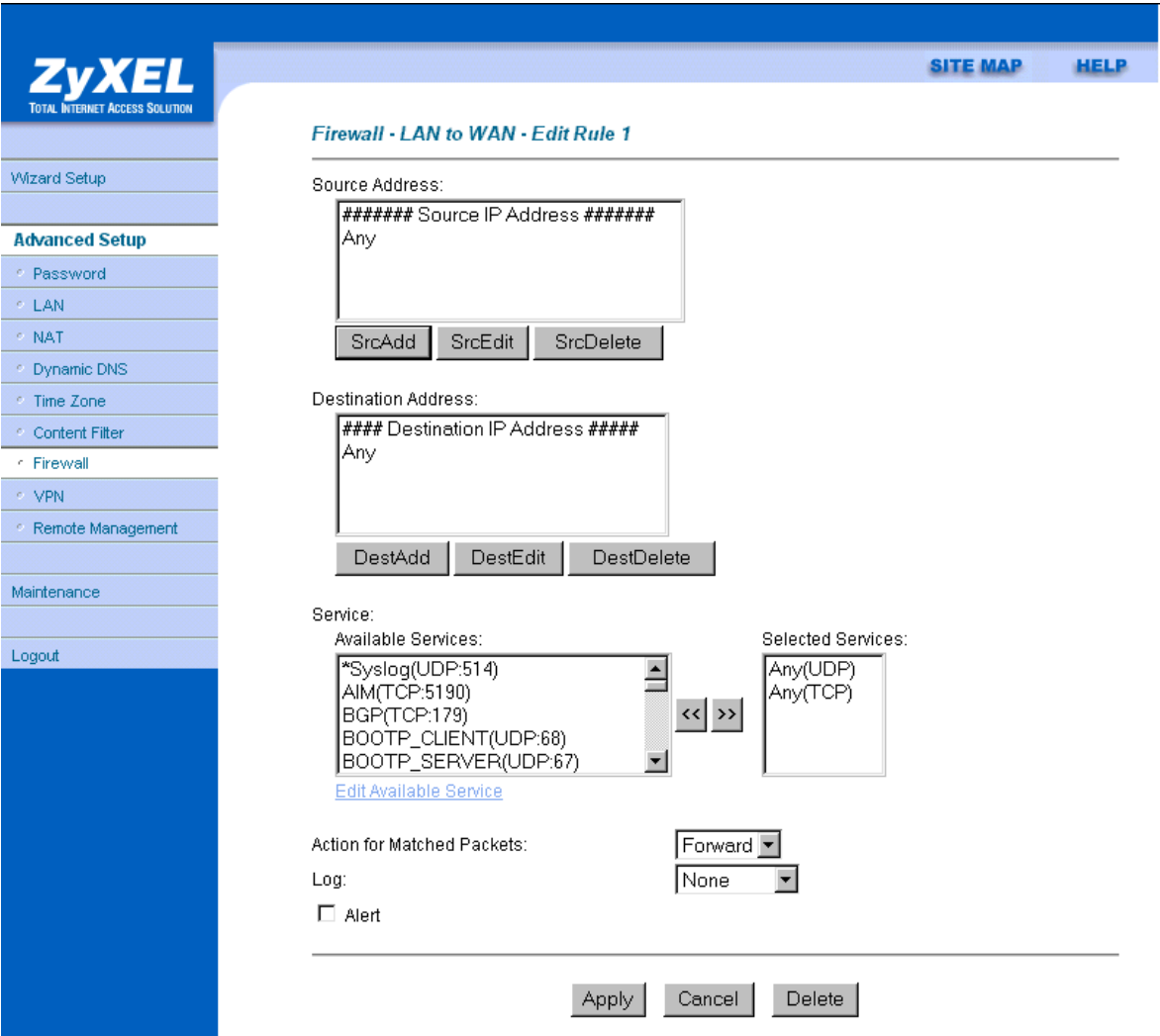


Figure 12-4 Creating/Editing A Firewall Rule

Table 12-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
Source Address	Click SrcAdd to add a new address, SrcEdit to edit	SrcAdd

Table 12-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
	an existing one or SrcDelete to delete one. Please see the next section for more information on adding and editing source addresses.	SrcEdit SrcDelete
Destination Address	Click DestAdd to add a new address, DestEdit to edit an existing one or DestDelete to delete one. Please see the following section on adding and editing destination addresses.	DestAdd DestEdit DestDelete
Services Available/Selected Services	Please see <i>Table 12-2</i> for more information on services available. Highlight a service from the Available Services box on the left, then click >> to add it to the Selected Services box on the right. To remove a service, highlight it in the Selected Services box on the right, then click << .	>> <<
Edit Available Service	Click this button to go to the list of available custom services.	
Action for Matched Packets	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that Block means the firewall silently discards the packet.	Block Forward
Log	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.	Match Not Match Both None
Alert	Check the Alert check box to determine that this rule generates an alert when the rule is matched.	
Click Back to return to the previous screen. Click Apply to save your customized settings and exit this screen. Click Cancel to exit this screen without saving. Use the Help icon to view field descriptions.		

12.5.2 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen. Either action displays the following screen.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

Wizard Setup

Advanced Setup

◦ Password

◦ LAN

◦ NAT

◦ Dynamic DNS

◦ Time Zone

◦ Content Filter

◦ Firewall

◦ VPN

◦ Remote Management

Maintenance

Logout

SITE MAPHELP

Firewall - LAN to WAN - Rule IP Config

Address Type:

Subnet Address

Start IP Address:

0.0.0.0

End IP Address:

0.0.0.0

Subnet Mask:

0.0.0.0

Apply

Reset

Figure 12-5 Adding/Editing Source and Destination Addresses

Table 12-4 Adding/Editing Source and Destination Addresses

FIELD	DESCRIPTION	OPTIONS
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box	Single Address Range Address Subnet Address Any Address
Start IP Address	Enter the single IP address or the starting IP address in a range here.	
End IP Address	Enter the ending IP address in a range here.	
Subnet Mask	Enter the subnet mask here, if applicable.	
Click Apply to save your customized settings and exit this screen. Click Reset to return to the previous configuration. Use the Help icon to view field descriptions.		

12.6 Timeout

The fields in the Timeout screens are the same for Local and Internet networks, so the discussion below refers to both.

12.6.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 11.4.1*. Click **Timeout** for either **Local Network** or **Internet**.

The screenshot displays the ZyXEL web interface for configuring firewall timeout settings. The left sidebar contains a navigation menu with options like Wizard Setup, Advanced Setup, Password, LAN, NAT, Dynamic DNS, Time Zone, Content Filter, Firewall, VPN, Remote Management, Maintenance, and Logout. The main content area is titled 'Firewall - LAN to WAN - Timeout' and includes a section for 'TCP Timeout Values' with input fields for Connection Timeout (30), FIN-Wait Timeout (60), and Idle Timeout (3600). Below this are fields for 'UDP Idle Timeout' (60) and 'ICMP Timeout' (60). At the bottom right, there are 'Back', 'Apply', and 'Reset' buttons.

Timeout Type	Value (sec)
TCP Connection Timeout	30
TCP FIN-Wait Timeout	60
TCP Idle Timeout	3600
UDP Idle Timeout	60
ICMP Timeout	60

Figure 12-6 Timeout Screen

Table 12-5 Timeout Menu

FIELD	DESCRIPTION	DEFAULT VALUE
TCP Timeout Values Connection Timeout	This is the length of time the Prestige waits for a TCP session to reach the established state before dropping the session.	30 seconds
FIN-Wait Timeout	This is the length of time a TCP session remains open after the firewall detects a FIN-exchange (indicating the end of the TCP session).	60 seconds
Idle Timeout	This is the length of time of inactivity a TCP connection remains open before the Prestige considers the connection closed.	3600 seconds (1 hour)
UDP Idle Timeout	This is the length of time of inactivity a UDP connection remains open before the Prestige considers the connection closed.	60 seconds
ICMP Timeout	This is the length of time an ICMP session waits for the ICMP response.	60 seconds
Click Back to return to the previous screen. Click Apply to save your customized settings and exit this screen. Click Reset to return to the previous configuration. Use the Help icon to view field descriptions.		

Chapter 13

Customized Services

This chapter covers creating, viewing and editing custom services.

13.1 Introduction

Configure customized services and port numbers not predefined by the Prestige (see *Figure 12-4*). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 12.5*. To configure a custom service, click **Edit Available Service** in an edit rule screen to bring up the following screen.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

Wizard Setup

Advanced Setup

- Password
- LAN
- NAT
- Dynamic DNS
- Time Zone
- Content Filter
- Firewall
- VPN
- Remote Management

Maintenance

Logout

SITE MAPHELP

Firewall - Customized Services

No.	Name	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Back

Figure 13-1 Customized Services

The next table describes the fields in this screen.

Table 13-1 Customized Services

FIELD	DESCRIPTION
Customized Services	
No.	This is the number of your customized port. Click a rule's number to edit the rule.
Name	This is the name of your customized port.
Protocol	This shows the IP protocol (TCP, UDP or Both) that defines your customized port.
Port	This is the port number or range that defines your customized port.
Use the Help icon for field descriptions. When you have finished viewing this screen, click another link to exit. Click Back to return to the previous screen.	

13.2 Creating/Editing A Customized Service

Click a rule number in the previous screen to create a new custom port or edit an existing one. This action displays the following screen.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

Wizard Setup

Advanced Setup

• Password

• LAN

• NAT

• Dynamic DNS

• Time Zone

• Content Filter

• Firewall

• VPN

• Remote Management

Maintenance

Logout

[SITE MAP](#)

[HELP](#)

Firewall - Customized Services - Config

Service Name:

Service Type:

TCP/UDP ▾

Port Configuration

Type:

☒ Single ☐ Range

Port Number:

0

 -

0

Back

Apply

Reset

Delete

Figure 13-2 Creating/Editing A Customized Service

The next table describes the fields in this screen.

Table 13-2 Creating/Editing A Custom Port

FIELD	DESCRIPTION	OPTIONS
Service Name	Enter a unique name for your custom port.	
Service Type	Choose the IP port (TCP , UDP or TCP/UDP) that defines your customized port from the drop down list box.	TCP UDP TCP/UDP

Table 13-2 Creating/Editing A Custom Port

FIELD	DESCRIPTION	OPTIONS
Port Configuration		
Type	Click Single to specify one port only or Range to specify a span of ports that define your customized service.	Single Range
Port Number	Enter a single port number or the range of port numbers that define your customized service.	
Click Back to return to the previous screen. When you have finished, click Apply to save your customized settings and exit this screen, Reset to return to the previously saved settings, Delete to remove this customized service. Click the Help icon for field descriptions.		

13.3 Example DHCP Negotiation and Syslog Connection from the Internet

The following are some Internet firewall rule examples that allow DHCP negotiation between the ISP and the Prestige and allow a syslog connection from the Internet. Follow the procedure shown next to first configure a custom port.

- Step 1.** Click **Rule Summary** under **Internet to Local Network Set**.
- Step 2.** Click a rule number to open the edit rule screen.
- Step 3.** Click **Any** in the Source Address box and then click **ScrDelete**.
- Step 4.** Click **ScrAdd** to open the Rule IP Config screen. Configure it as follows and click **Apply**.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

[SITE MAP](#) [HELP](#)

Wizard Setup

Advanced Setup

- Password
- LAN
- NAT
- Dynamic DNS
- Time Zone
- Content Filter
- Firewall
- VPN
- Remote Management

Maintenance

Logout

Firewall - WAN to LAN - Rule IP Config

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Figure 13-3 Configure Source IP

Step 5. Click **Edit Available Service** in the edit rule screen and then click a rule number to bring up the **Firewall Customized Services Config** screen. Configure as follows.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

[SITE MAP](#) [HELP](#)

Firewall - Customized Services - Config

Service Name:

Service Type:

Port Configuration

Type: ☒ Single ☐ Range

Port Number: -

Figure 13-4 Customized Service for Syslog

Customized services show up with an “*” before their names in the Services list box and the Rule Summary list box. Click Apply after you’ve created your customized service.

Step 5. Follow the procedures outlined earlier in this chapter to configure all your rules. Configure the rule configuration screen like the one below and apply it.

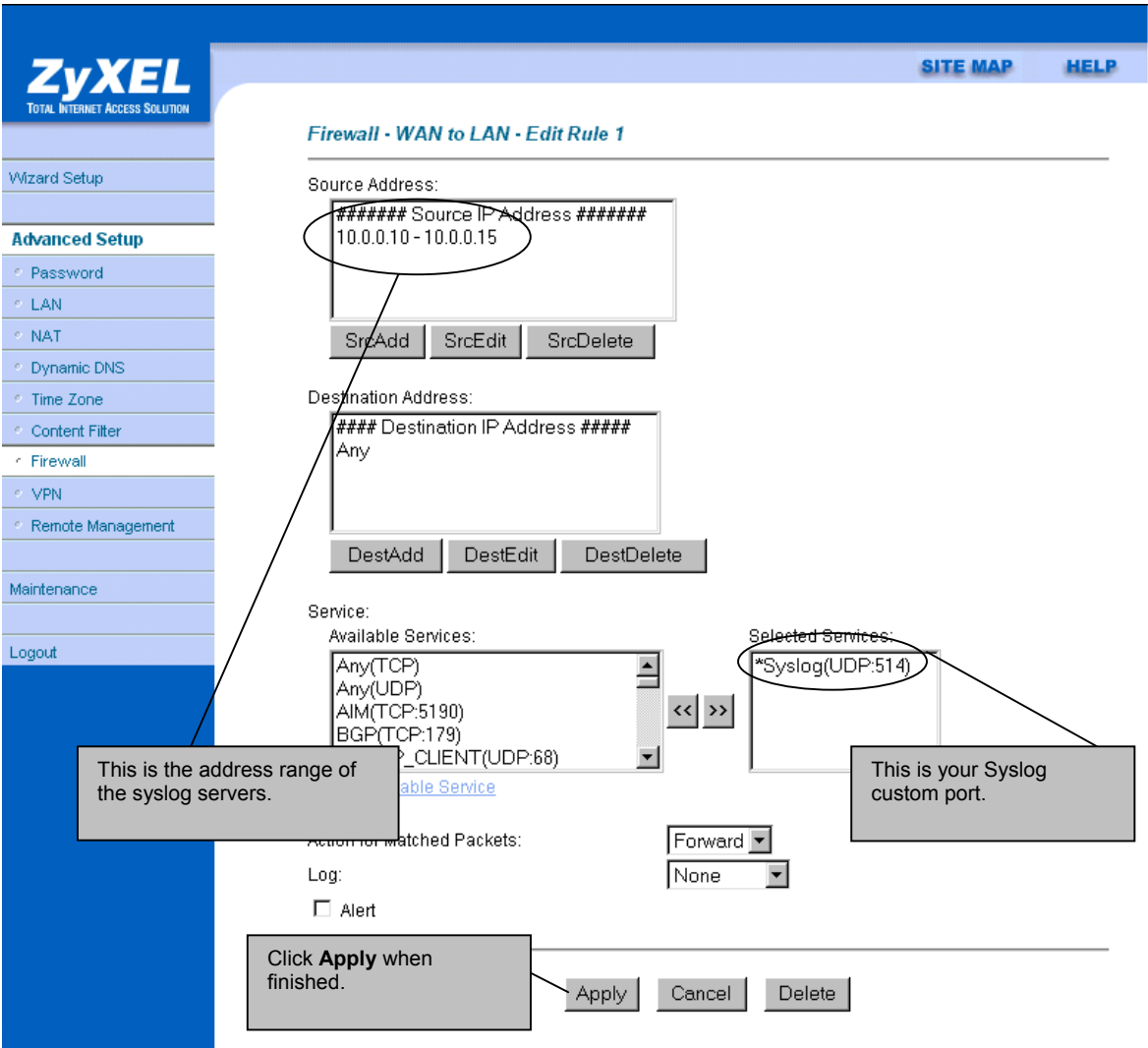


Figure 13-5 Syslog Rule Configuration

Step 6. On completing the configuration procedure for these Internet firewall rules, the **Rule Summary** screen should look like the following. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the Prestige.

ZyXEL
TOTAL INTERNET ACCESS SOLUTION
[SITE MAP](#) [HELP](#)

Wizard Setup

Advanced Setup

- Password
- LAN
- NAT
- Dynamic DNS
- Time Zone
- Content Filter
- Firewall
- VPN
- Remote Management

Maintenance

Logout

Firewall - WAN to LAN - Rule Summary

The default action for packets not matching following rules: Block

☒ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	10.0.0.10 - 10.0.0.15	Any	*Syslog(UDP:514)	Forward	None
2					
3					
4					
5					
6					
7					
8					
9					
10					

Rules Reorder: Move rule number
1
to rule number
1
Move

Back
Apply
Reset

This rule allows a syslog connection from the WAN.

Click **Apply** to save your settings back to the Prestige.

Figure 13-6 Example Rule Summary

Chapter 14

Logs

This chapter contains information about using the log screen to view the results of the rules you have configured.

14.1 Log Screen

When you configure a new rule you also have the option to log events that match, don't match (or both) this rule (see *Figure 12-4*). Click **Logs** to bring up the next screen. Firewall logs may also be viewed in SMT Menu 21.3 (see *section 10.3*) or via syslog (SMT **Menu 24.3.2 - System Maintenance - UNIX Syslog**). Syslog is an industry standard protocol used for capturing log information for devices on a network. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.

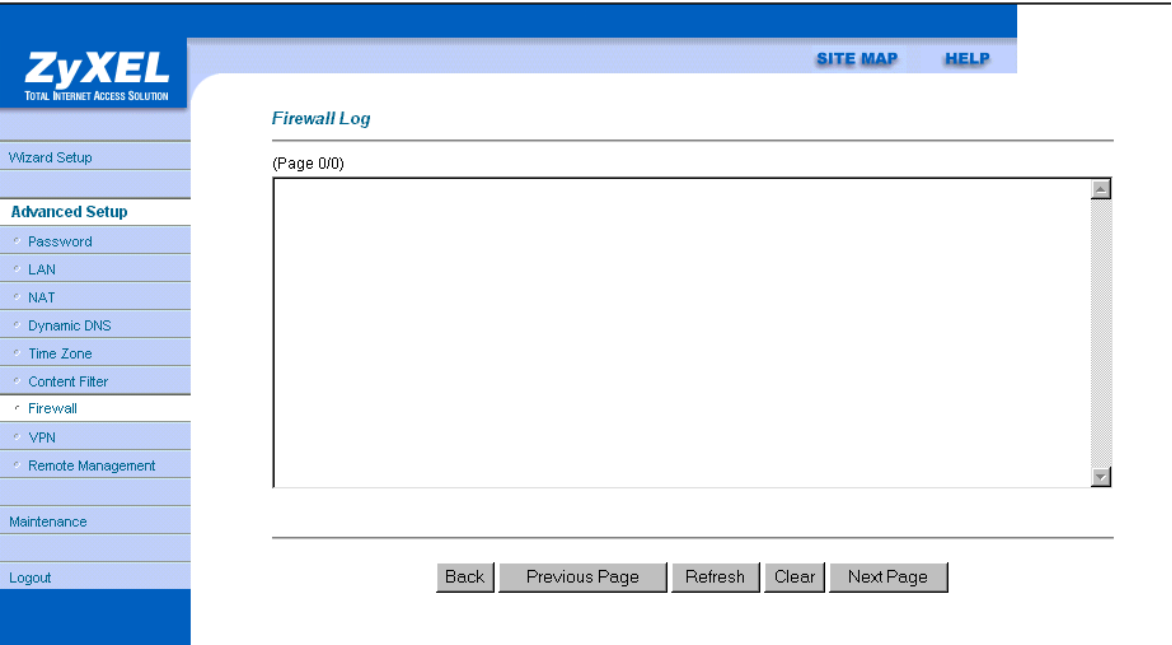


Figure 14-1 Log Screen

Table 14-1 Log Screen

FIELD	DESCRIPTION	EXAMPLES
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd:mm:yy e.g., Jan 1 0
		hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as:	From and To IP addresses
		protocol and port numbers.
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood. <i>Chapter 9</i> has more detailed discussion of what these attacks mean.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). "None" means that no action is dictated by this rule.	Block, Forward or None
Click Back to return to the previous screen. Click Previous Page or Next Page to view other pages in your log. Click Refresh to renew the log screen or Clear to clear all the logs. Click the Help icon for field descriptions.		

Chapter 15

Content Filtering

This chapter provides a brief overview of content filtering using the web embedded configurator.

Internet content filtering allows schools and businesses to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URLs and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Advanced**, then **Content Filter** to display the Content Filter menus. Use the help icon for more detailed information on the fields in each screen.

15.1 Keyword

Configure the Prestige to block Web sites that use certain keywords in their URL.

15.2 Schedule

The Prestige allows the administrator to define time periods and days during which content filtering should be enabled.

15.3 Trusted

Configure this screen to exclude a computer or a range of computers from content filtering.

15.4 Logs

This screen displays the results of your content filter policies

Part IV:

ADVANCED MANAGEMENT

This part discusses Filtering, SNMP, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, Remote Management and IP Policy Routing.

Chapter 16

Filter Configuration

This chapter shows you how to create and apply filters.

16.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

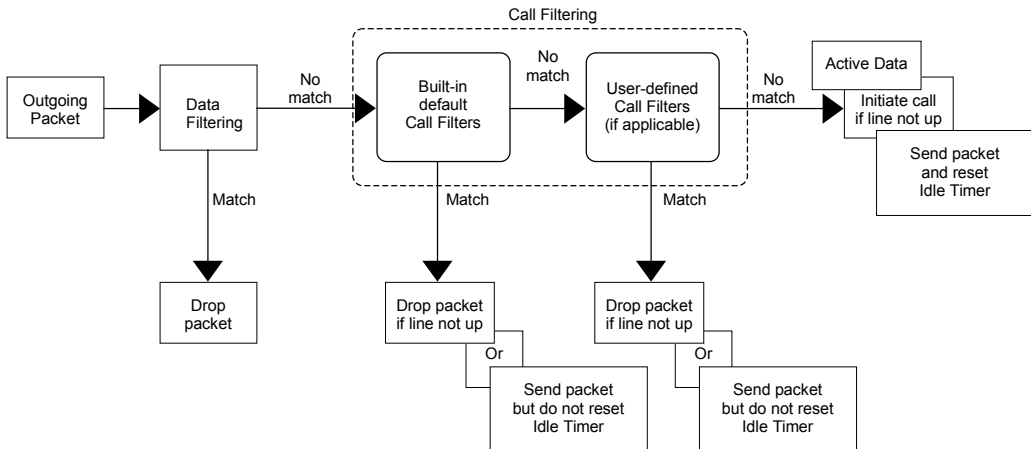


Figure 16-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

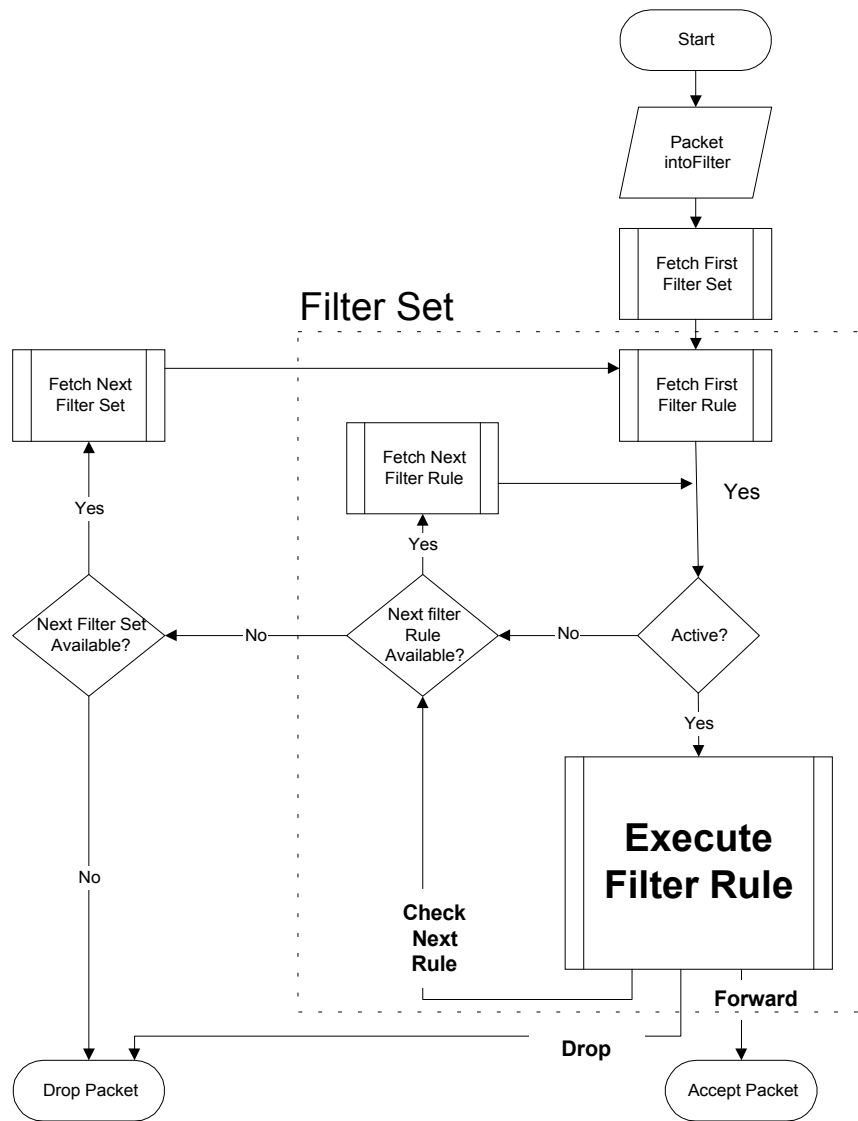


Figure 16-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

16.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 in the main menu to open menu 21.

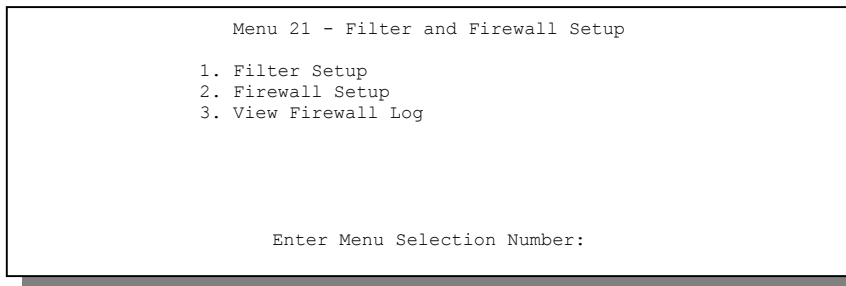


Figure 16-4 Menu 21 — Filter and Firewall Setup

Step 2. Enter 1 to bring up the following menu.

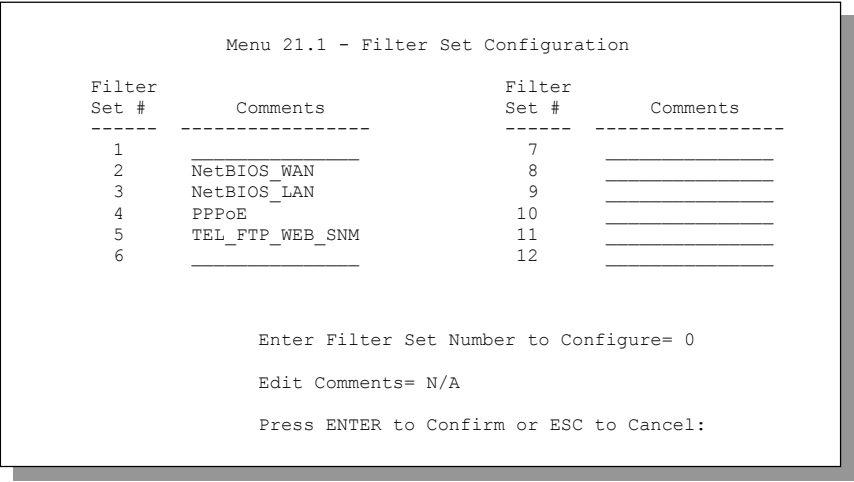


Figure 16-5 Menu 21.1 — Filter Set Configuration

- Step 3.** Select the filter set you wish to configure (1-12) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

Menu 21.1.2 - Filter Rules Summary									
#	A	Type	Filter Rules					M m n	

1	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137		N	D N
2	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138		N	D N
3	Y	IP	Pr=6,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139		N	D N
4	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=137		N	D N
5	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=138		N	D N
6	Y	IP	Pr=17,	SA=0.0.0.0,	DA=0.0.0.0,	DP=139		N	D F
Enter Filter Rule Number (1-6) to Configure:									

Figure 16-6 NetBIOS_WAN Filter Rules Summary

Menu 21.1.3 - Filter Rules Summary										
#	A	Type	Filter Rules					M	m	n
-	-	-	-----					-	-	-
1	Y	IP	Pr=17,	SA=0.0.0.0,	SP=137,	DA=0.0.0.0,	DP=53	N	D	F
2	N									
3	N									
4	N									
5	N									
6	N									
Enter Filter Rule Number (1-6) to Configure:										

Figure 16-7 NetBIOS_LAN Filter Rules Summary

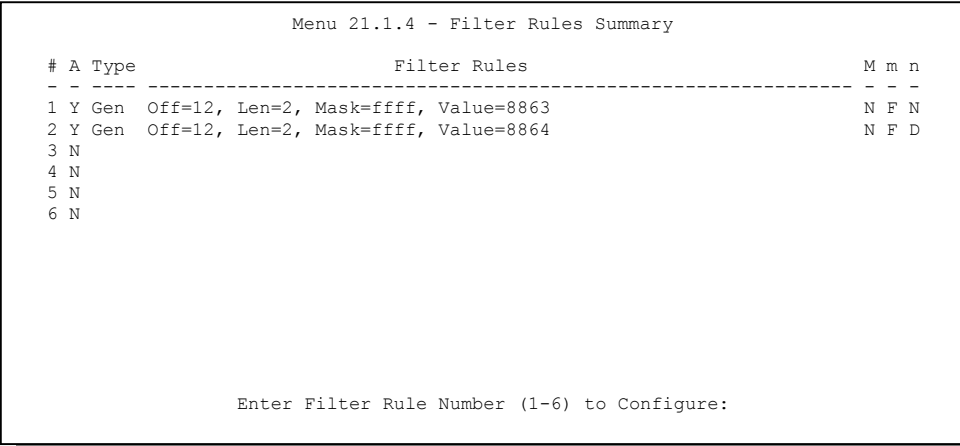


Figure 16-8 PPPoE Filter Rules Summary

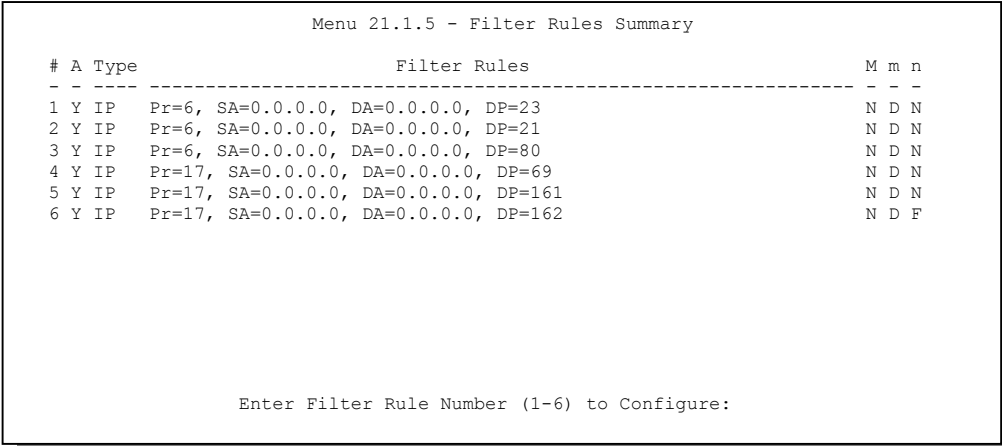


Figure 16-9 TEL_FTP_WEB_SNM Filter Rules Summary

16.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in the previous menus.

Table 16-1 Filter Rules Summary Menu Abbreviations

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 16-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
Off	Offset
Len	Length

16.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

16.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.7.1 – TCP/IP Filter Rule**, as shown next.

```
Menu 21.1.7.1 - TCP/IP Filter Rule
Filter #: 4,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6          IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 137
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
TCP Estab= No
More= No              Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 16-10 Menu 21.1.7.1 — TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 16-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	7,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are TCP/IP Filter Rule or Generic Filter Rule .	TCP/IP Filter Rule
Active	Use [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate the filter rule.	No (default)
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If Yes , the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	No (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port # . Choices are None , Less , Greater , Equal or Not Equal .	None
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the Source: IP Addr field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port # field. Choices are None , Less , Greater , Equal or Not Equal .	None
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If Yes , the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	No (default)

FIELD	DESCRIPTION	EXAMPLE
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A.	No (default)
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only packets that match the rule parameters will be logged. Action Not Matched – Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None
Action Matched	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

The following figure illustrates the logic flow of an IP filter.

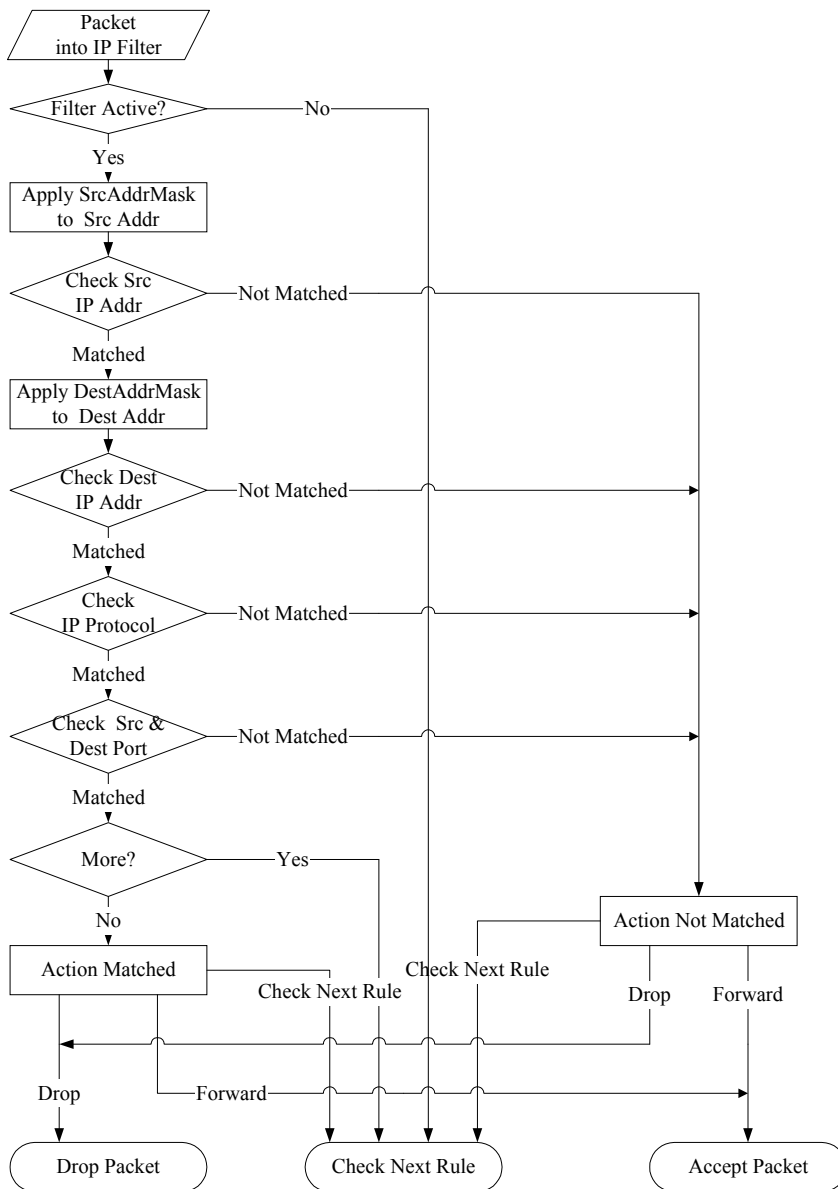


Figure 16-11 Executing an IP Filter

16.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21.1, for example 8. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.5.1 – Generic Filter Rule**, as shown in the following figure.

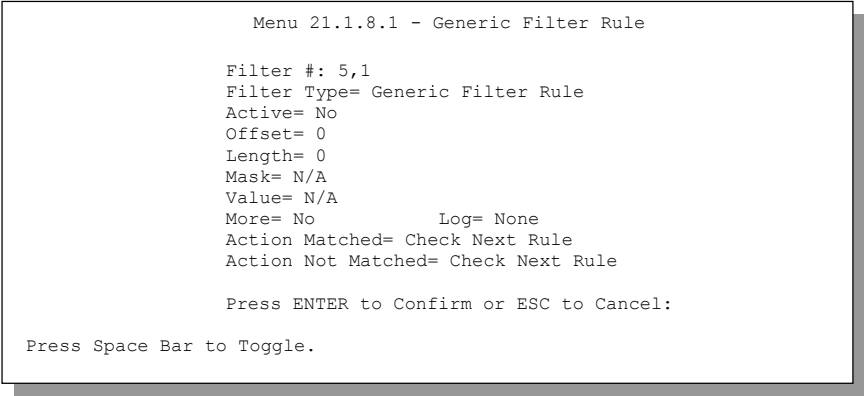


Figure 16-12 Menu 21.1.5.1 — Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 16-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	8,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are Generic Filter Rule or TCP/IP Filter Rule .	Generic Filter Rule
Active	Select Yes to turn on or No to turn off the filter rule.	No (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	No (default)
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only matching packets and rules will be logged. Action Not Matched – Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None
Action Matched	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

16.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

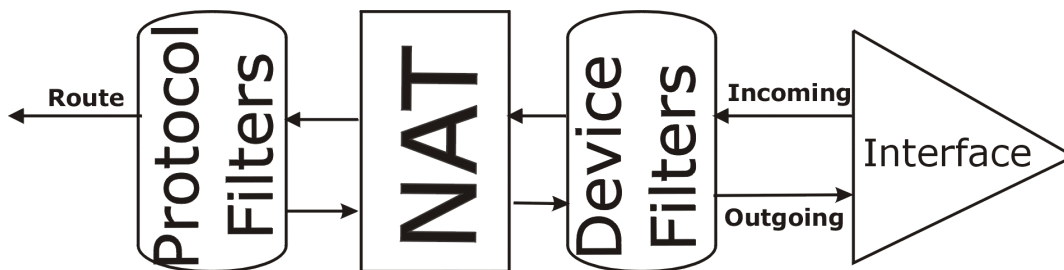


Figure 16-13 Protocol and Device Filter Sets

16.5 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige. See the *included disk* for example filters.

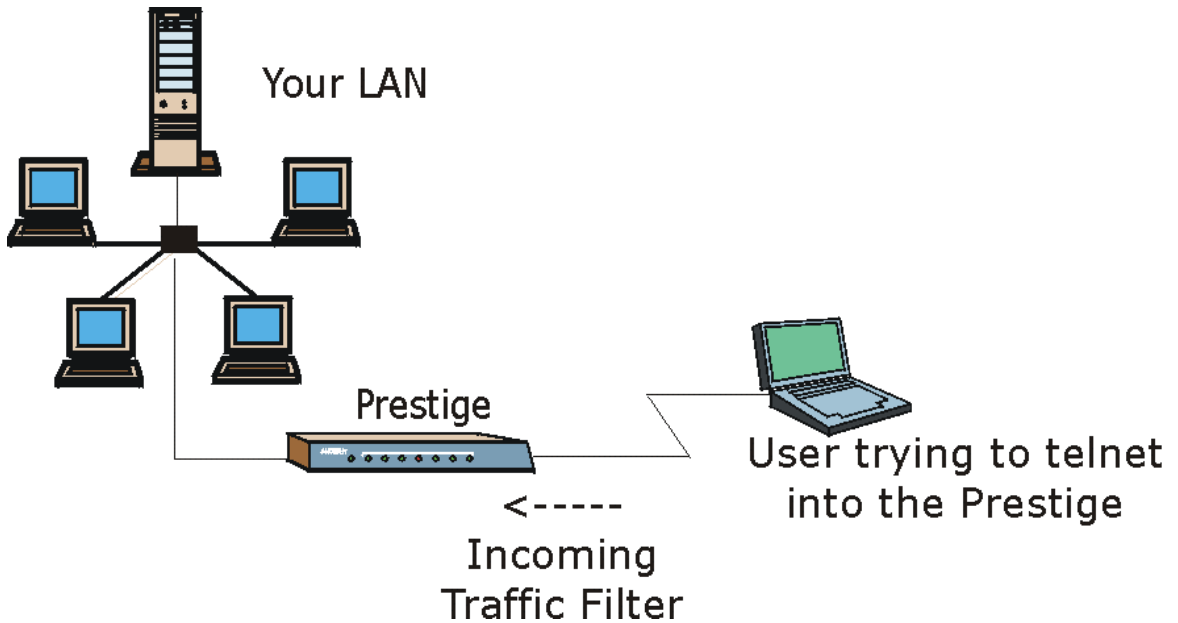


Figure 16-14 Sample Telnet Filter

- Step 1.** Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- Step 2.** Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- Step 3.** Enter the index of the filter set you wish to configure (say 4) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.9 - Filter Rules Summary**.
- Step 6.** Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Menu 21.1.9.1 - TCP/IP Filter Rule

Filter #: 9,1

Filter Type= TCP/IP Filter Rule

Active= Yes

IP Protocol= 6

IP Source Route= No

Destination: IP Addr= 0.0.0.0

IP Mask= 0.0.0.0

Port # = 23

Port # Comp= Equal

Source: IP Addr= 0.0.0.0

IP Mask= 0.0.0.0

Port # =

Port # Comp= None

TCP Estab= No

More= No

Log= None

Action Matched= Drop

Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:

Press [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See RFC-1060 for port numbers of well-known services.

Select **Equal** here as we are looking for packets going to port 23 only.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

There are no more rules to check.

Figure 16-15 Sample Filter — Menu 21.1.9.1

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

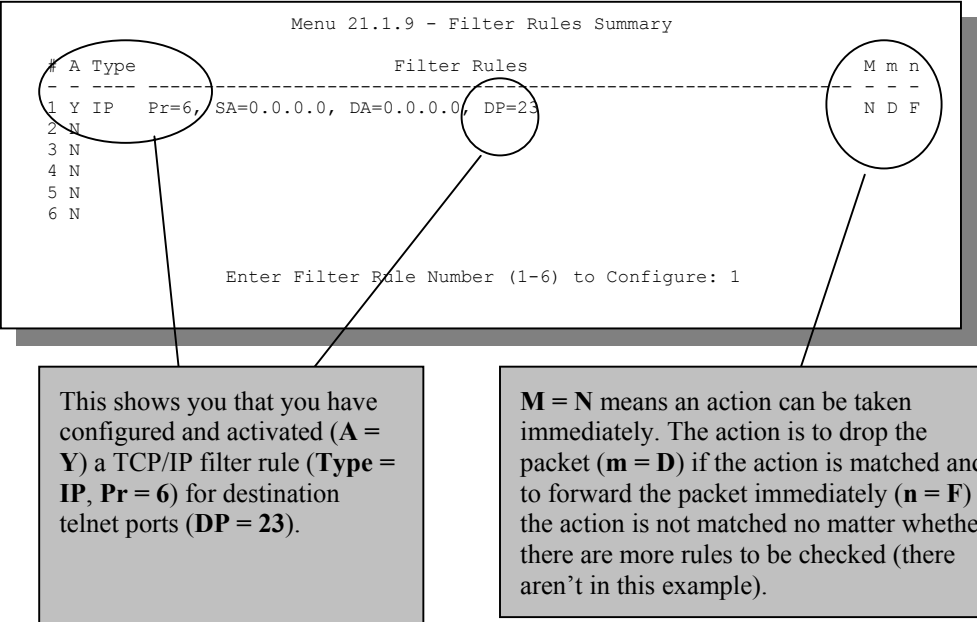


Figure 16-16 Sample Filter Rules Summary — Menu 21.1.9

After you have created the filter set, you must apply it.

- Step 1.** Type 11 in the main menu to go to menu 11 and type the remote node number to edit.
- Step 2.** Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].
- Step 3.** This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

16.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 16-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

16.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

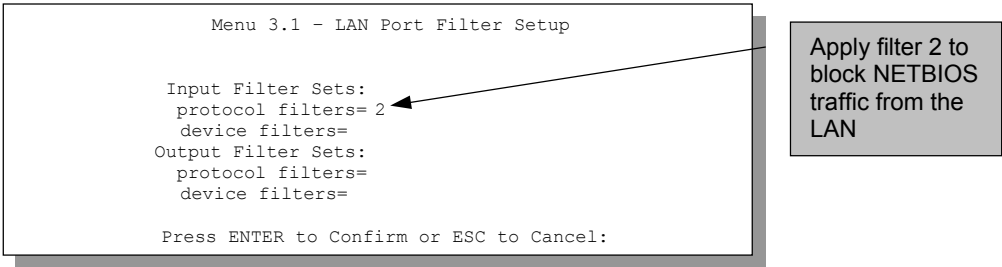


Figure 16-17 Filtering Ethernet Traffic

16.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas.

For PPPoE encapsulation, you have the option of specifying remote node call filter sets. Insert the factory default filter set, NetBIOS_WAN, in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

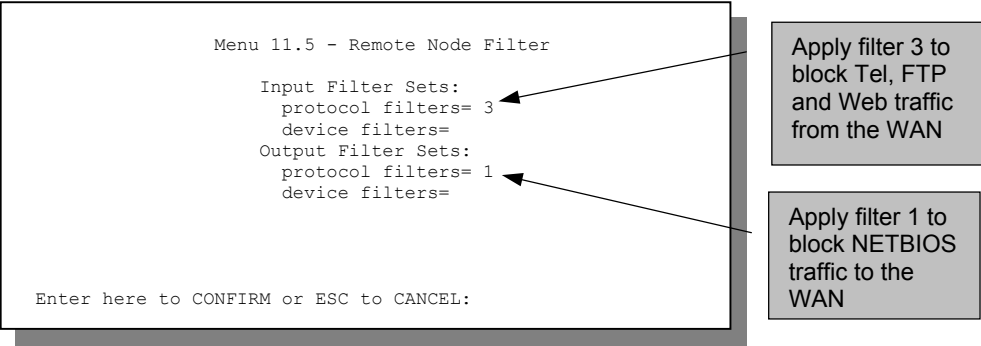


Figure 16-18 Filtering Remote Node Traffic

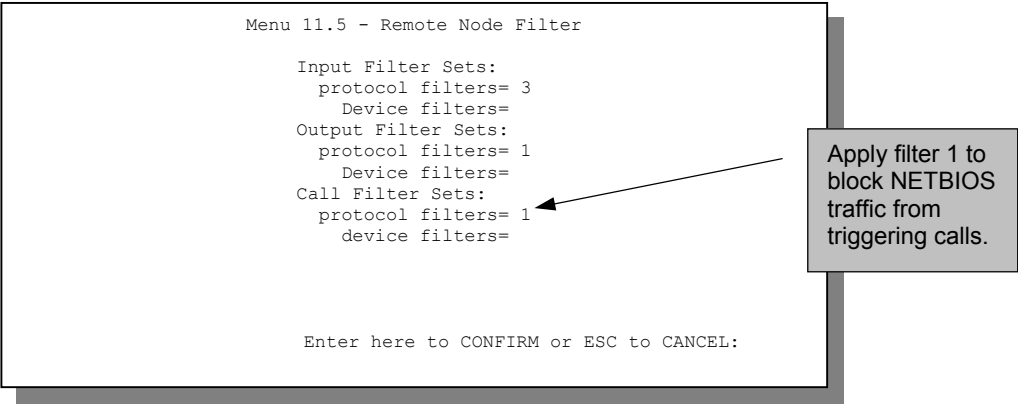


Figure 16-19 Filtering Remote Node Traffic with PPPoE

Chapter 17

SNMP Configuration

This chapter explains SNMP Configuration menu 22.

SNMP is only available if TCP/IP is configured.

17.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

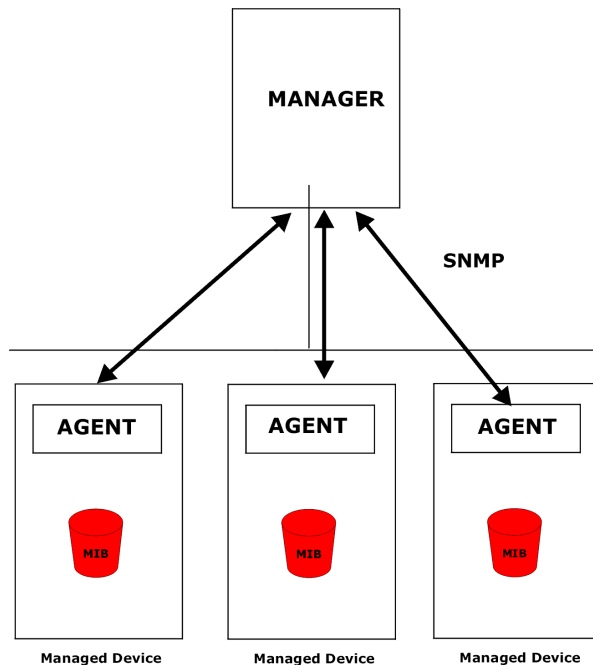


Figure 17-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

17.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

17.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 - SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

```
Menu 22 - SNMP Configuration

SNMP:
Get Community= public
Set Community= public
Trusted Hgst= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
```

Figure 17-2 Menu 22 — SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 17-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

17.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 17-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent with the port number.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 17-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
...	...
13	12
14	xDSL

Chapter 18

System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

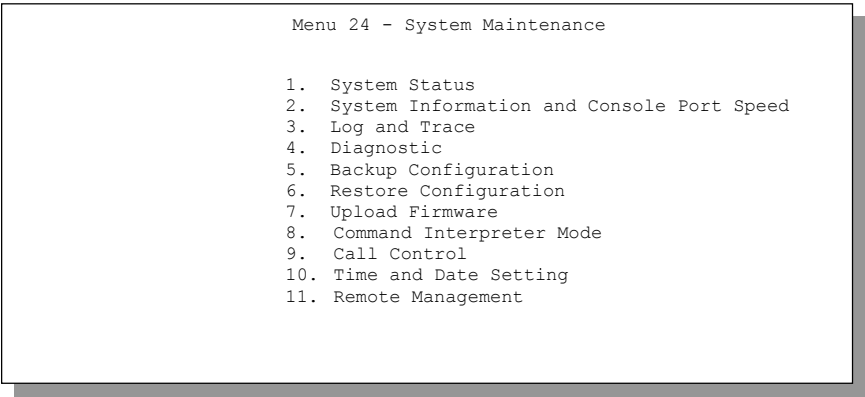


Figure 18-1 Menu 24 — System Maintenance

18.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your G.SHDSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 – System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Typing 1 resets the counters, [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are READ-ONLY and meant for diagnostic purposes.

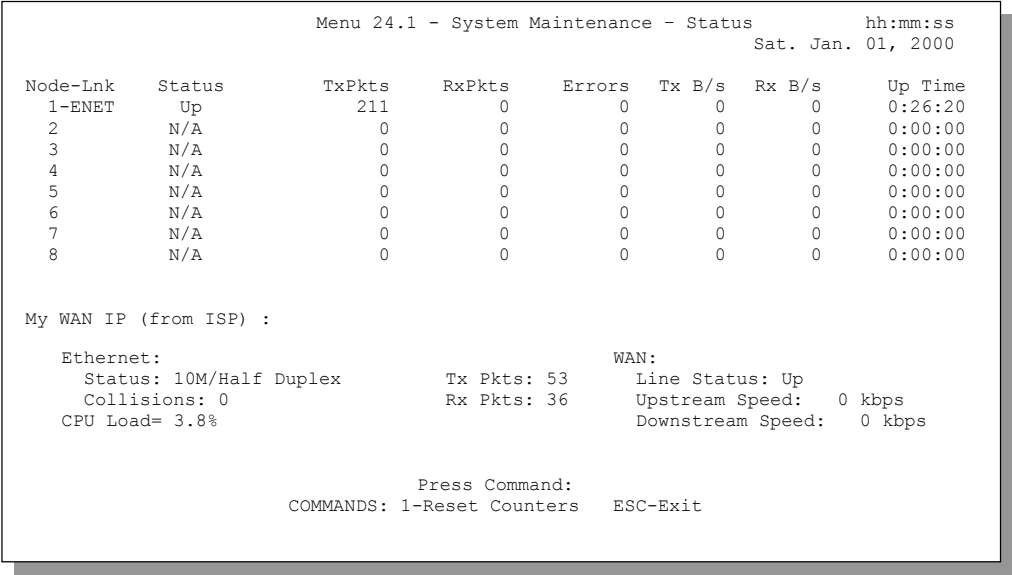


Figure 18-2 Menu 24.1 — System Maintenance — Status

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status**.

Table 18-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPPoA, ENET, 1483.
Status	Shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
My WAN IP (from ISP)	The IP address of the ISP remote node.
Ethernet	Shows statistics for the LAN.

FIELD	DESCRIPTION
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	Shows statistics for the WAN.
Line Status	Shows the current status of the xDSL line, which can be Up or Down.
Upstream Speed	Shows the transfer rate of traffic going out from the Prestige to the WAN.
Downstream Speed	Shows the transfer rate of traffic coming into the Prestige from the WAN.
CPU Load	Specifies the percentage of CPU utilization.

18.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

- Step 1.** Enter 24 to go to **Menu 24 – System Maintenance**.
- Step 2.** Enter 2 to open **Menu 24.2 – System Information and Console Port Speed**.
- Step 3.** From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information and Console Port Speed
1. System Information
2. Console Port Speed

Please enter selection:
```

Figure 18-3 Menu 24.2 — System Information and Console Port Speed

18.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V3.40(FN.0)b13 | 4/22/2002
ADSL Chipset Vendor: Alcatel, Version 3.8.163
Standard: Multi-Mode

LAN
Ethernet Address: 00:a0:c5:01:23:45
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
```

Figure 18-4 Menu 24.2.1 — System Maintenance — Information

Table 18-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

18.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200bps. Use [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

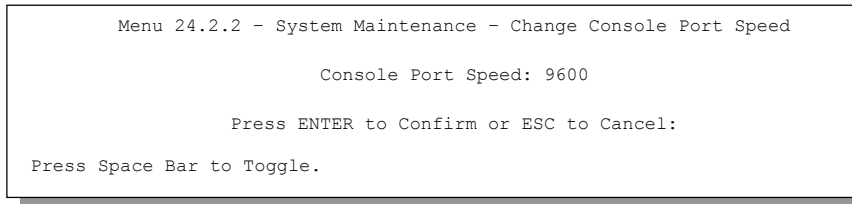


Figure 18-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed

18.3 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

18.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- Step 1.** Type 24 in the main menu to display **Menu 24 – System Maintenance**.
- Step 2.** From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

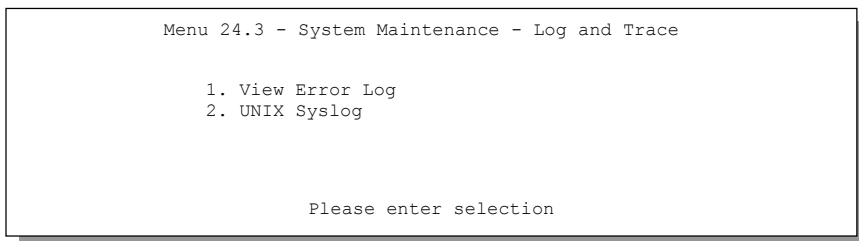


Figure 18-6 Menu 24.3 — System Maintenance — Log and Trace

- Step 3.** Enter 1 from **Menu 24.3 – System Maintenance – Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
59 Thu Jan 01 00:00:03 1970 PP0f INFO LAN promiscuous mode <0>
60 Thu Jan 01 00:00:03 1970 PP00 -WARN SNMP TRAP 0: cold start
61 Thu Jan 01 00:00:03 1970 PP00 INFO main: init completed
62 Thu Jan 01 00:00:19 1970 PP00 INFO SMT Session Begin
63 Thu Jan 01 00:00:24 1970 PP0a WARN MPOA Link Down
Clear Error Log (y/n):
```

Figure 18-7 Sample Error and Information Messages

18.3.2 Syslog and Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 – System Maintenance – UNIX Syslog**, as shown next.

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

Types:
CDR= No
Packet triggered= No
Filter Log= No
PPP Log= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 18-8 Menu 24.3.2 — System Maintenance — Syslog and Accounting

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 18-3 System Maintenance Menu — Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to Yes .
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to Yes .
Filter Log	No filters are logged when this field is set to No . Filters with the individual filter Log Filter field set to Yes are logged when this field is set to Yes .
PPP Log	PPP events are logged when this field is set to Yes .

The following are examples of the four types of syslog messages sent by the Prestige:

1 - CDR
SdcmSyslogSend (SYSLOG CDR, SYSLOG INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
2 - Packet Triggered
SdcmSyslogSend (SYSLOG PKTTRI, SYSLOG NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxxxx...x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f70717273 74

Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
3 - Filter Log
SdcmSyslogSend (SYSLOG FILLOG, SYSLOG NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
4 - PPP Log
SdcmSyslogSend (SYSLOG PPPLOG, SYSLOG NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCF / CBCP / CCF / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing

18.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

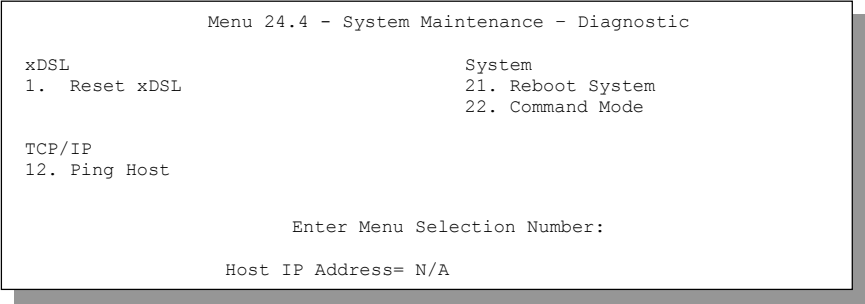


Figure 18-9 Menu 24.4 — System Maintenance — Diagnostic

Follow the procedure next to get to Diagnostic:

- Step 1.** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- Step 2.** From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for and the connections.

Table 18-4 System Maintenance Menu — Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

18.5 Command Interpreter Mode

This option allows you to enter the command interpreter mode. A list of valid commands can be found by typing help or ? at the command prompt.

```
Copyright (c) 1994 - 2002 ZYXEL
ras> ?
Valid commands are:
sys          exit          device      ether
wan          poe           config     ip
ipsec        ppp           bridge    hdap
```

Figure 18-10 Command Mode

Chapter 19

Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

19.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

Table 19-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the Prestige.	*.bin

19.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

19.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

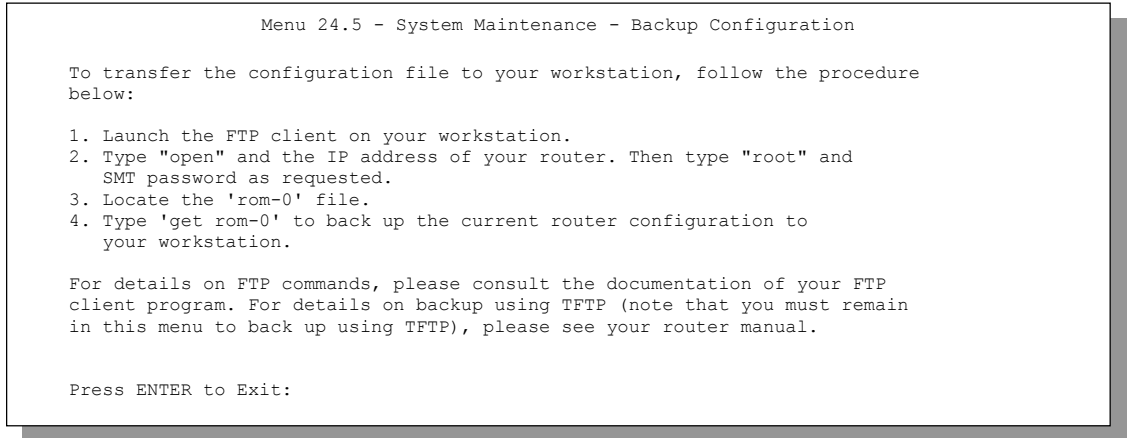


Figure 19-1 Telnet in Menu 24.5

19.2.2 Using the FTP Command from the Command Line

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open", followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Use "get" to transfer files from the Prestige to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the Prestige to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter "quit" to exit the ftp prompt.

19.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 19-2 FTP Session Example

19.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 19-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

19.2.5 Remote Management Limitations

TFTP, FTP and Telnet from the LAN or WAN will not work when:

- 1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2. You have disabled that service in menu 24.11.

3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there is already a web session.

19.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

- Step 1.** Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the Prestige to the computer and “binary” to set binary transfer mode.

19.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige IP address, “get” transfers the file source on the Prestige (rom-0, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

19.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 19-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the Prestige and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 19.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

19.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter “y” at the following screen.

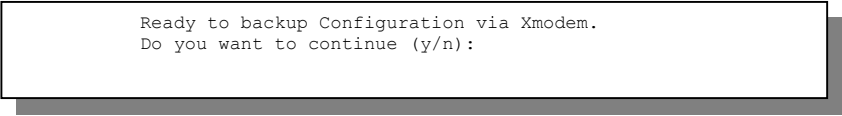


Figure 19-3 System Maintenance — Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

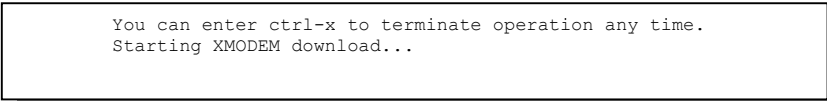


Figure 19-4 System Maintenance — Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

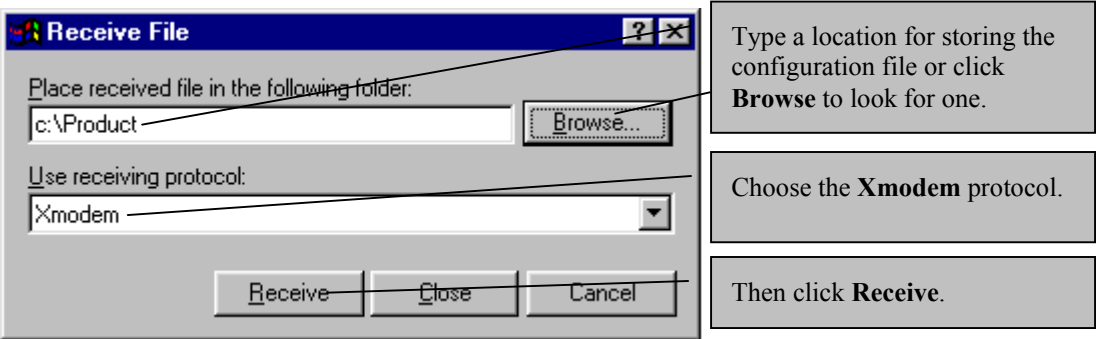


Figure 19-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

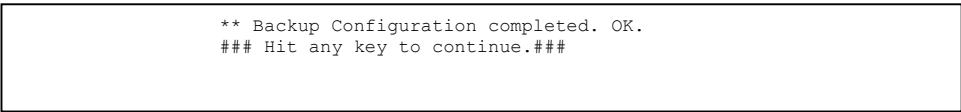


Figure 19-6 Successful Backup Confirmation Screen

19.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring a previously saved configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESTART.

19.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of your backup configuration file on your workstation and rom-0 is the remote file name on the router. This restores the configuration to your router.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP client program. For details on backup using TFTP (note that you must remain in this menu to back up using TFTP), please see your router manual.

Press ENTER to Exit:

Figure 19-7 Telnet into Menu 24.6

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open", followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Find the "rom" file (on your computer) that you want to restore to your Prestige.

- Step 7.** Use “put” to transfer files from the Prestige to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.
- Step 8.** Enter “quit” to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

19.3.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 19-8 Restore Using FTP Session Example

Refer to *section 19.2.5* to read about configurations that disallow TFTP and FTP from the WAN.

19.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- Step 1.** Display menu 24.6 and enter “y” at the following screen.

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 19-9 System Maintenance — Restore Configuration

- Step 2.** The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCC
```

Figure 19-10 System Maintenance — Starting Xmodem Download Screen

- Step 3.** Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

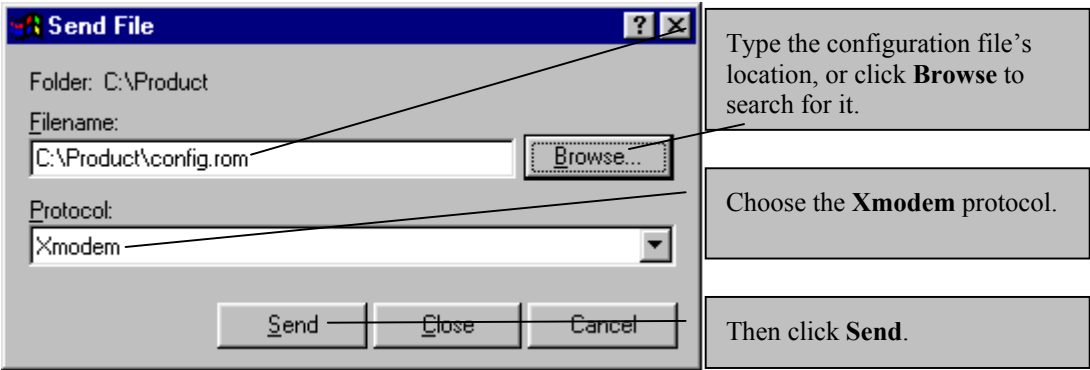


Figure 19-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

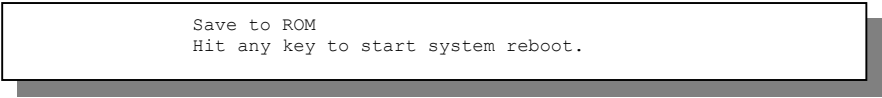


Figure 19-12 Successful Restoration Confirmation Screen

19.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

19.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name of your firmware upgrade file on your workstation and "ras" is the remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading system firmware using TFTP (note that you must remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:

Figure 19-13 Telnet Into Menu 24.7.1 — Upload System Firmware

19.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and SMT password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of your system configuration file on your workstation, which will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration file process is complete.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading system firmware using TFTP (note that you must remain on this menu to upload system firmware using TFTP), please see your manual.

Press ENTER to Exit:

Figure 19-14 Telnet Into Menu 24.7.2 — System Maintenance

To upload the firmware and the configuration file, follow these examples

19.4.3 FTP File Upload Command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 6.** Use “put” to transfer files from the computer to the Prestige, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter “quit” to exit the ftp prompt.

19.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 19-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 19.2.5* to read about configurations that disallow TFTP and FTP over WAN.

19.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- Step 1.** Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the Prestige to the computer, “put” the other way around, and “binary” to set binary transfer mode.

19.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

19.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

19.4.8 Uploading Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, then follow the instructions as shown in the following screen.

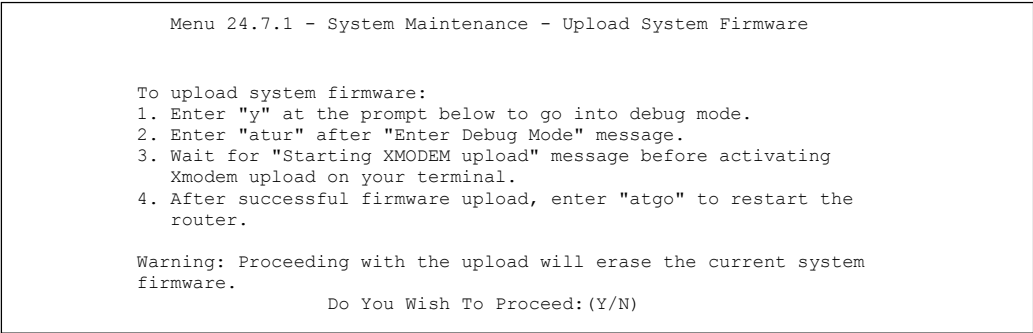


Figure 19-16 Menu 24.7.1 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

19.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

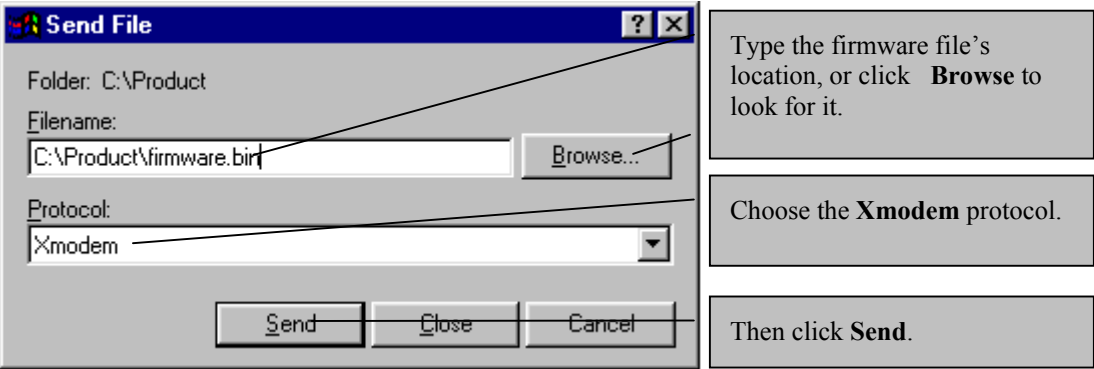


Figure 19-17 Example Xmodem Upload

After the firmware upload process has completed, the Prestige will automatically restart.

19.4.10 Uploading Configuration File Via Console Port

- Step 1.** Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:

1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the system.

Warning:

1. Proceeding with the upload will erase the current configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is restarted; please adjust your terminal's speed accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console port speed will be reset to 9600 bps and the password to "1234".

Do You Wish To Proceed: (Y/N)

Figure 19-18 Menu 24.7.2 as seen using the Console Port

- Step 2.** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Enter "atgo" to restart the Prestige.

19.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

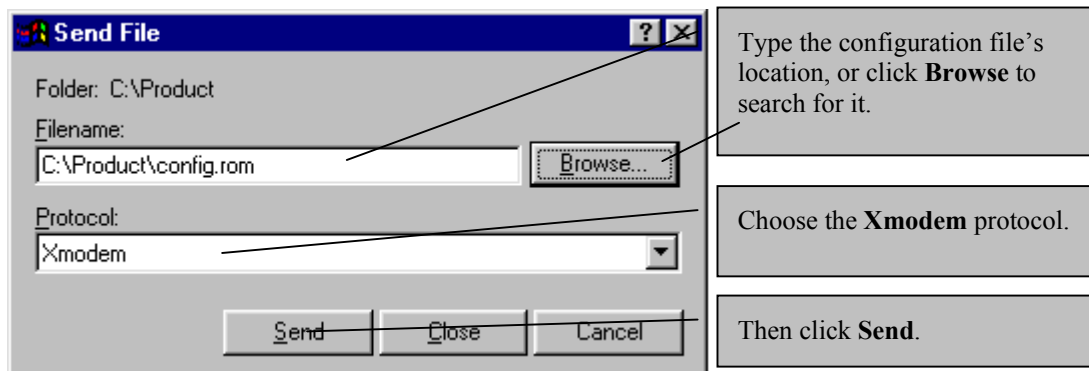


Figure 19-19 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

Chapter 20

System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.10.

20.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Firmware Update
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Figure 20-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys                exit                device                ether
wan                poe                 config               ip
ipsec              ppp                 bridge              hdap
ras>
```

Figure 20-2 Valid Commands

20.2 Call Control Support

The Prestige provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
```

Figure 20-3 Call Control

20.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

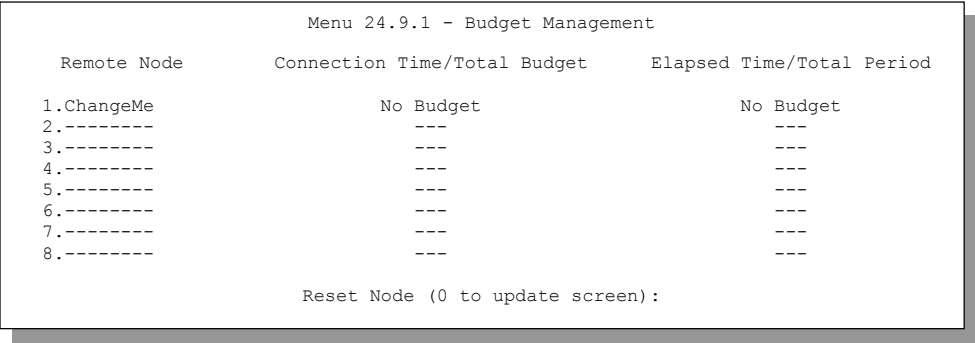


Figure 20-4 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 20-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

20.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

Figure 20-5 Menu 24 — System Maintenance

Then enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server Address= N/A

Current Time:                00 : 00 : 00
New Time (hh:mm:ss):        11 : 23 : 16

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2001 - 03 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):          01 - 00
End Date (mm_dd):            01 - 00

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 20-6 Menu 24.10 System Maintenance — Time and Date Setting

Table 20-2 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	<p>Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None. The default, enter the time manually.</p>
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose Yes .
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

20.3.1 Resetting the Time

The Prestige resets the time in three instances:

- i. On leaving menu 24.10 after making changes.
- ii. When the Prestige starts up, if there is a time server configured in menu 24.10.
- iii. 24-hour intervals after starting.

Chapter 21

Remote Management

This chapter covers remote management found in SMT menu 24.11.

21.1 About Telnet Configuration

Before the Prestige is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your Prestige is configured, you can use Telnet to configure it remotely as shown below.

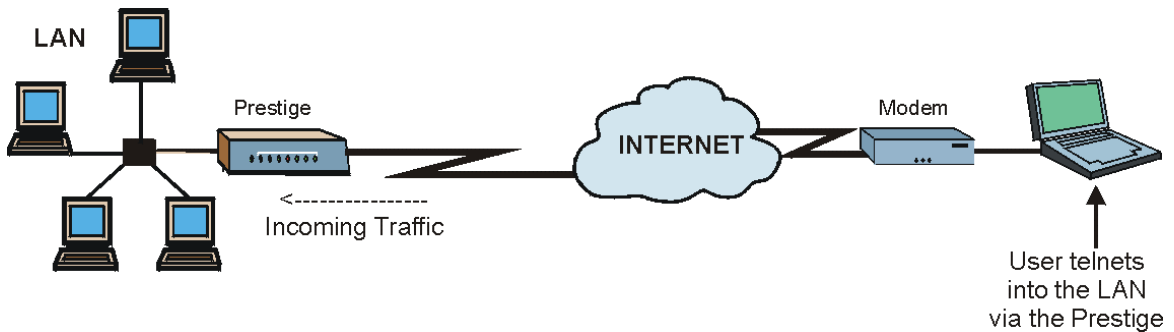


Figure 21-1 Telnet Configuration on a TCP/IP Network

21.2 Telnet Under NAT

When Network Address Translation (NAT) is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the Prestige via telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the Prestige using its inside LAN IP address. If no inside server is specified, telnetting to the NAT's IP address will connect to the Prestige directly.

21.3 Telnet Capabilities

21.3.1 Single Administrator

To prevent confusion and discrepancy on the configuration, your Prestige only allows one administrator to log in at any time. Your Prestige also gives priority to the console port over telnet. If you have already connected to your Prestige via telnet, you will be logged out if another user logs in to the Prestige via the console port.

21.4 FTP

You can upload and download the Prestige's firmware and configuration files using FTP, please see the *Firmware and Configuration File Maintenance* chapter for details. To use this feature, your computer must have an FTP client.

21.5 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the *Using the Prestige Web Configurator* chapter for an introduction to the web configurator.

21.6 Remote Management

Remote management control is for managing Telnet, Web and FTP services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your Prestige from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

Choosing WAN only or ALL (LAN & WAN) automatically creates a hole in the firewall for the server type specified.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

```
Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 21-2 Menu 24.11 – Remote Management Control

Table 21-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
TELNET Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: LAN only , WAN only , ALL or Disable .	LAN Only (default)
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Enter an IP address to restrict access to a client with a matching IP address. This field is N/A when the Server Access field is set to Disable .	0.0.0.0 (default)
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

21.6.1 Remote Management Limitations

Remote management from the LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there is already a web session.
7. When enabled, the firewall allows remote management from the LAN, but blocks remote management from the WAN (unless you configure a firewall rule to allow it).

21.7 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

21.8 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys studio` has been changed on the command line.

Chapter 22

IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

22.1 Introduction

Traditionally, routing is based on the destination address only and the Prestige takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

22.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

22.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

22.4 IP Routing Policy Setup

Menu 25 lists all the policies that are defined.

Menu 25 - IP Routing Policy Setup

Policy Set #	Name	Policy Set #	Name
1	test	7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Policy Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

Figure 22-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

- Step 1.** Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup**.
- Step 2.** Type the index of the policy set that you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.

Menu 25.1 - IP Routing Policy Setup

A

Criteria/Action

1

Y

SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
SP=20-25,DP=20-25,P=6,T=NM,PR=0

|GW=192.168.1.1,T=MT,PR=0

2

N

3

N

4

N

5

N

6

N

Enter Policy Rule Number (1-6) to Configure:

Figure 22-2 Menu 25.1 — Sample IP Routing Policy Setup

Table 22-1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17...)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
	GW	Gateway IP address
Action	T	Outgoing Type of service
	P	Outgoing Precedence
	NM	Normal
Service	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

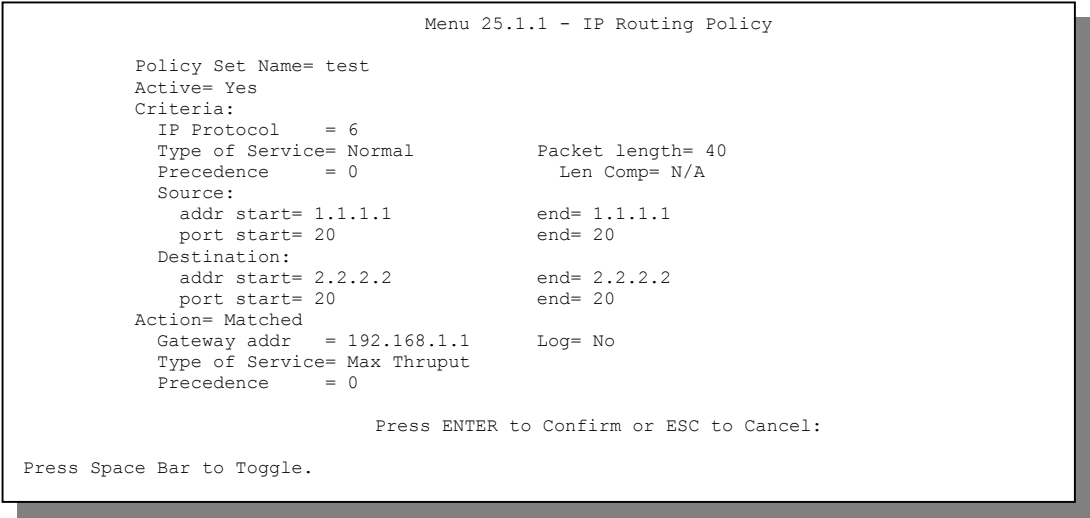


Figure 22-3 IP Routing Policy

Table 22-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in Menu 25 – IP Routing Policy Setup .
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate the policy.
Criteria	
IP Protocol	IP layer 4 protocol, for example, UDP, TCP, ICMP , etc.
Type of Service	Prioritize incoming network traffic by choosing from Don't Care, Normal, Min Delay, Max Thruput, Min Cost or Max Reliable .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from 0 to 7 or Don't Care .
Packet Length	Type the length of incoming packets (in bytes). The operators in the Len Comp (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal, Not Equal, Less, Greater, Less or Equal or Greater or Equal .

FIELD	DESCRIPTION
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched .
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing No Change , Normal , Min Delay , Max Thruput , Max Reliable or Min Cost .
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or No Change .
Log	Press [SPACE BAR] and then [ENTER] to select Yes to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

22.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

22.5.1 Ethernet IP Policies

From **Menu 3 – Ethernet Setup**, type 2 to go to **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

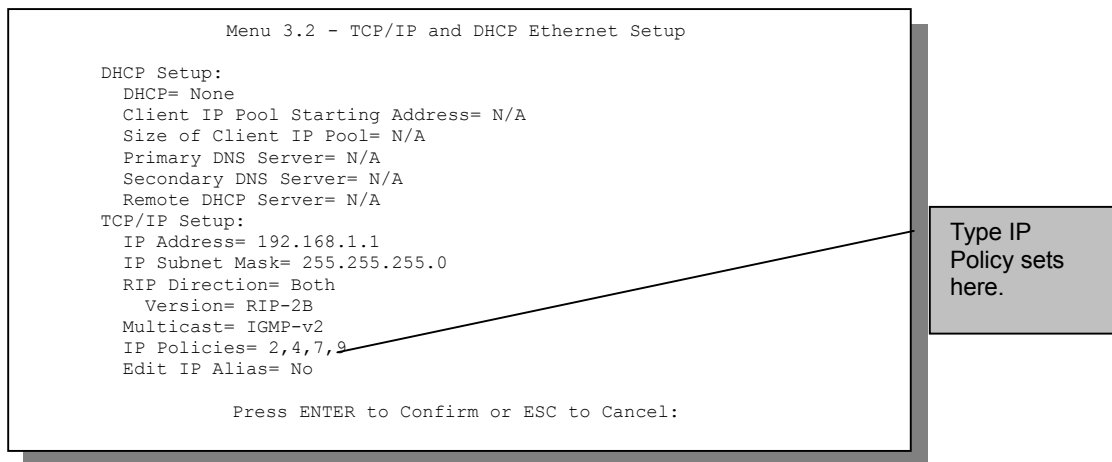


Figure 22-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

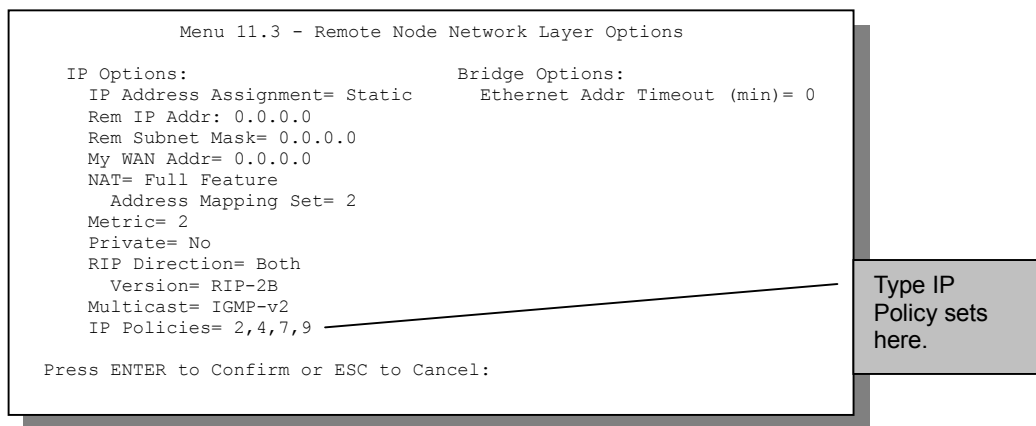


Figure 22-5 Menu 11.3 — Remote Node Network Layer Options

22.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

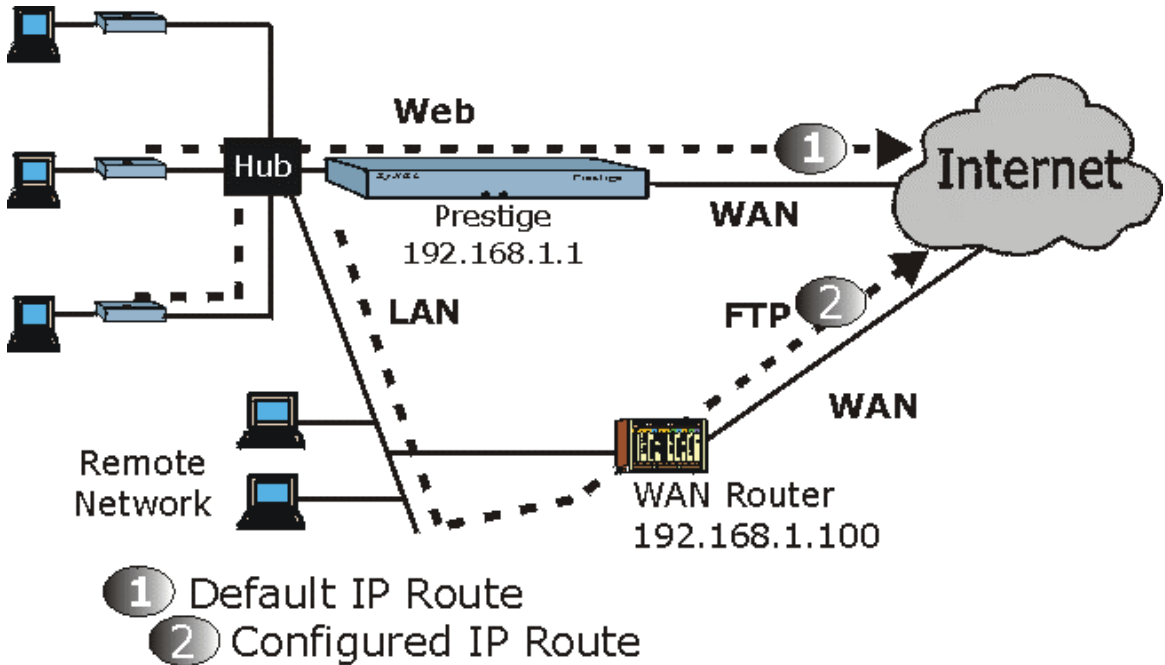


Figure 22-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 - IP Routing Policy** as shown next.

```
Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care
  Precedence      = Don't Care
Source:
  addr start= 192.168.1.2
  port start= 0
Destination:
  addr start= 0.0.0.0
  port start= 80
Action= Matched
Gateway addr  = 192.168.1.1
Type of Service= No Change
Precedence   = No Change
Packet length= 10
Len Comp= N/A
end= 192.168.1.64
end= N/A
end= N/A
end= 80
Log= No

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 22-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```
Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2

Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care
  Precedence       = Don't Care
  Packet length= 10
  Len Comp= N/A
Source:
  addr start= 0.0.0.0
  port start= 0
  end= N/A
  end= N/A
Destination:
  addr start= 0.0.0.0
  port start= 20
  end= N/A
  end= 21
Action= Matched
Gateway addr =192.168.1.100
Type of Service= No Change
Precedence    = No Change
Log= No

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 22-8 IP Routing Policy

- Step 6.** Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.
- Step 7.** Apply both policy sets in menu 3.2 as shown next.

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 22-9 Applying IP Policies

Part V:

Call Scheduling, VPN/IPSec and Internal SPTGEN

Part V provides information about Call Scheduling, VPN/IPSec and Internal SPTGEN.

Chapter 23

Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

23.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder that lets you specify times to record programs. You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

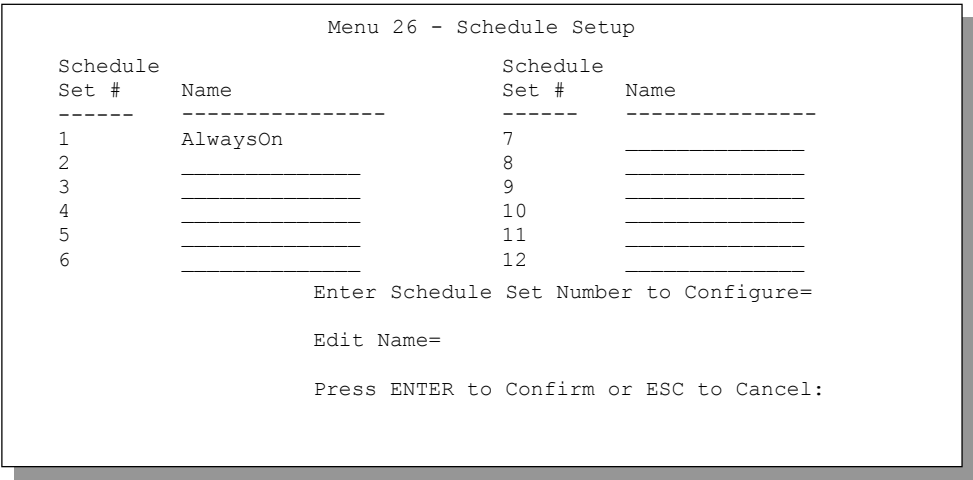


Figure 23-1 Menu 26 - Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can configure up to twelve schedule sets and apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] or [DELETE] in the Edit Name field.

To set up a schedule set select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

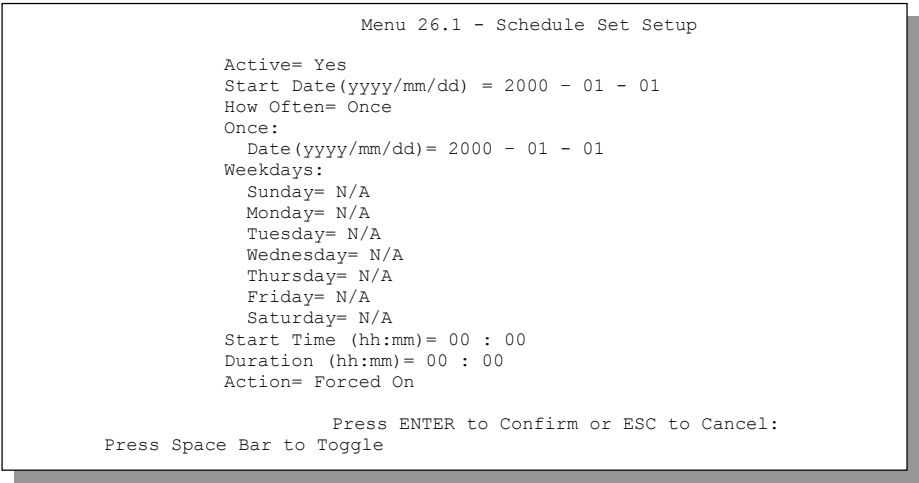


Figure 23-2 Schedule Set Setup

If a connection has already been established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 23-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] to toggle between Yes and No . Choose Yes and press [ENTER] to activate the schedule set.	Yes/No
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] to toggle between Once and Weekly . Both these options are mutually exclusive. If Once is selected, then all weekday settings are N/A . When Once is selected, the schedule rule deletes automatically after the scheduled time elapses.	Once/Weekly
Once: Date	If you selected Once in the How Often field above, then enter the date the set should activate here in year-month-date format.	
Weekday: Day	If you selected Weekly in the How Often field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select Yes , then press [ENTER].	Yes No N/A

Table 23-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTIONS
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	
Action	<p>Forced On means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>Enable Dial-On-Demand means that this schedule permits a demand call on the line.</p> <p>Disable Dial-On-Demand means that this schedule prevents a demand call on the line.</p>	<p>Forced On</p> <p>Forced Down</p> <p>Enable Dial-On-Demand</p> <p>Disable Dial-On-Demand</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter **11** from the Main Menu and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe
Active= Yes

Encapsulation= PPPoE
Multiplexing= LLC-based
Service Name=
Incoming:
 Rem Login=
 Rem Password= *****

Outgoing:
 My Login= ?
 My Password= ?
 Authen= CHAP/PAP

Route= IP
Bridge= No

Edit IP/Bridge= No
Edit ATM Options= No

Telco Option:
 Allocated Budget(min)= 0
 Period(hr)= 0
 Schedule Sets= 2,4,6,8
 Nailed-Up Connection= No

Session Options:
 Edit Filter Sets= No
 Idle Timeout(sec)= 0

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

Apply your schedule sets here.

Figure 23-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to 4 schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Chapter 24

Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

24.1 Introduction

24.1.1 VPN

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

24.1.2 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

24.1.3 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

24.1.4 Other Terminology

➤ Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms "ciphertext" to plaintext. Decryption also requires a key.

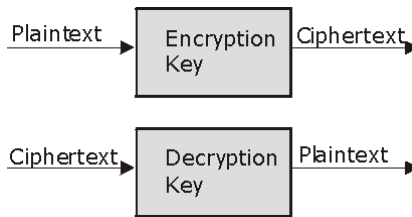


Figure 24-1 Encryption and Decryption

➤ **Data Confidentiality**

The IPSec sender can encrypt packets before transmitting them across a network.

➤ **Data Integrity**

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

➤ **Data Origin Authentication**

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

24.1.5 VPN Applications

The Prestige supports two active Security Associations (SAs) at a time.

➤ **Linking Two or More Private Networks Together**

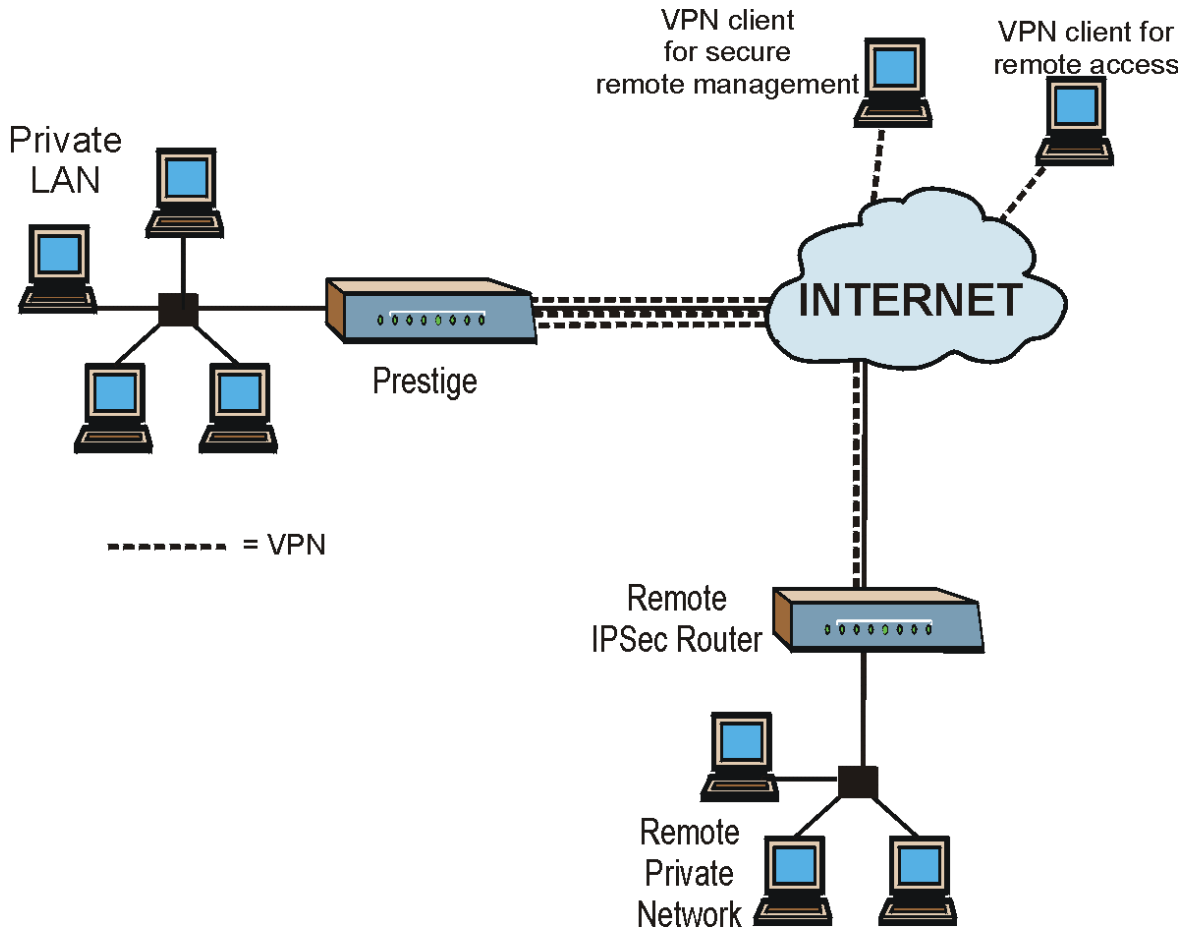
Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

➤ **Accessing Network Resources When NAT Is Enabled**

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

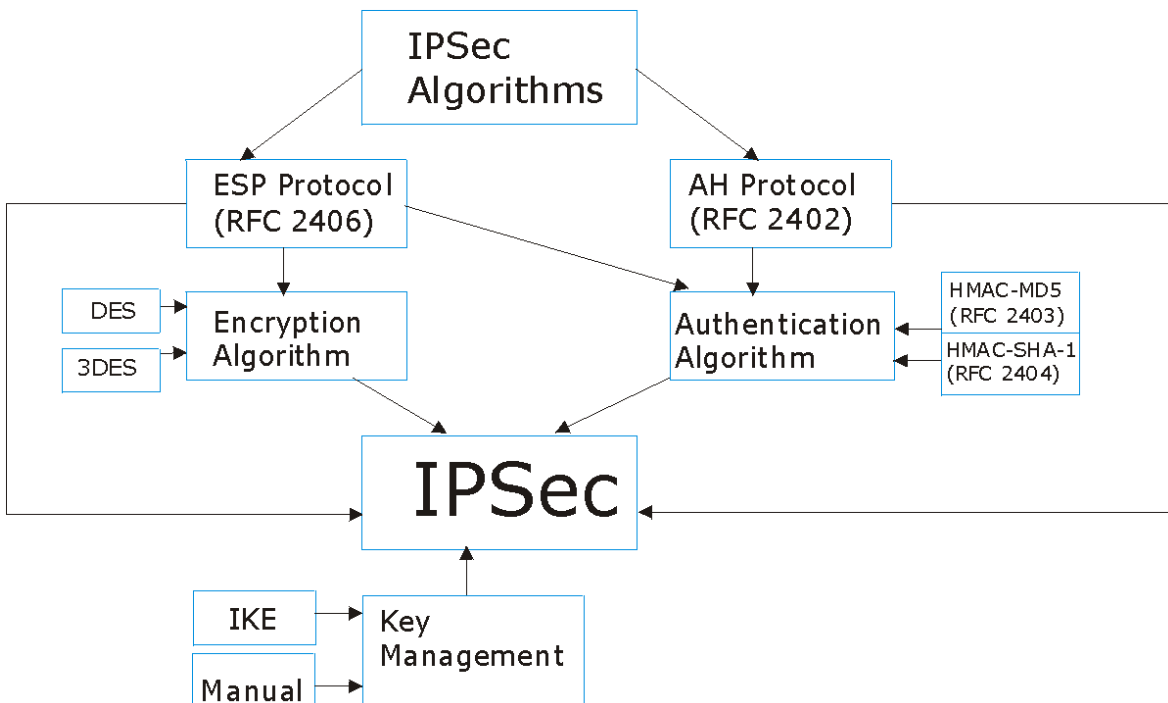
➤ **Unsupported IP Applications**

A VPN tunnel may be created to add support for unsupported emerging IP applications.

**Figure 24-2 VPN Application**

24.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 24-3 IPSec Architecture**

24.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *section 25.2* for more information.

24.2.2 Key Management

Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN. Please see *sections 25.5* and *25.6* for more information.

24.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

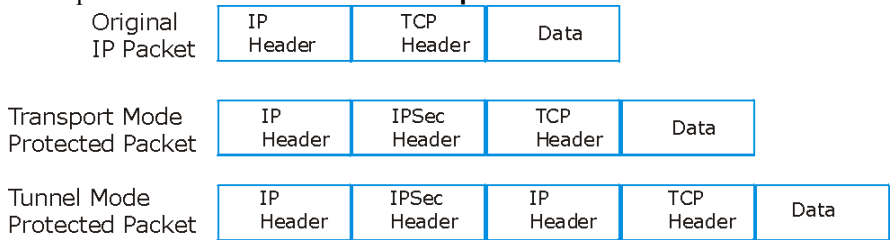


Figure 24-4 Transport and Tunnel Mode IPSec Encapsulation

24.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

24.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header:** The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

24.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Prestige. NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 24-1 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Chapter 25

VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

25.1 VPN/IPSec Setup

The VPN/IPSec main SMT menu has three main submenus.

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.
3. View the IPSec connection log in menu 27.4. This menu is also useful for troubleshooting.

This is an overview of the VPN menu tree.

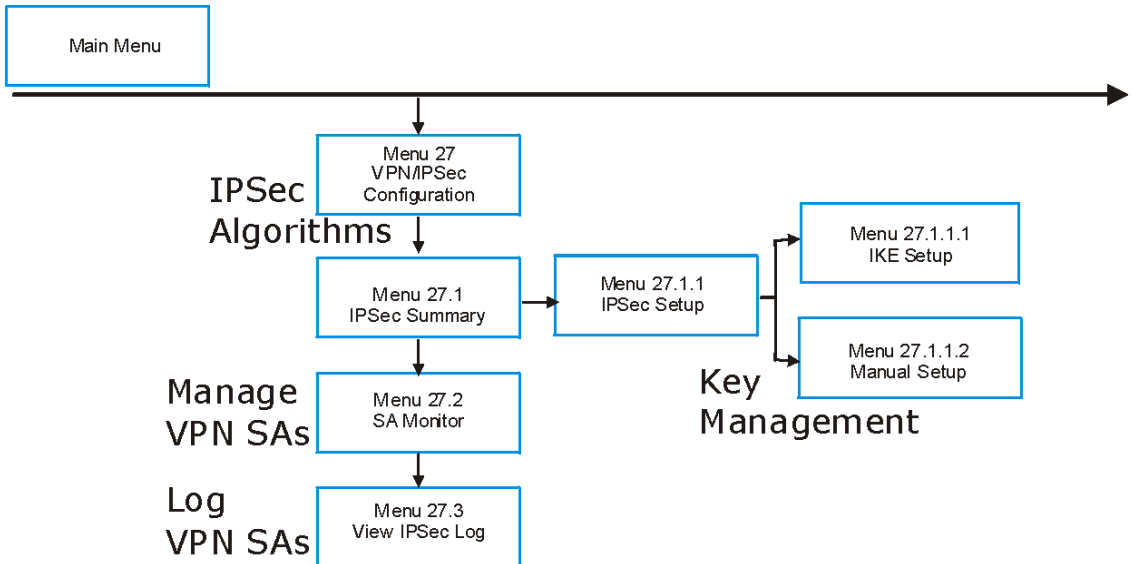


Figure 25-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).

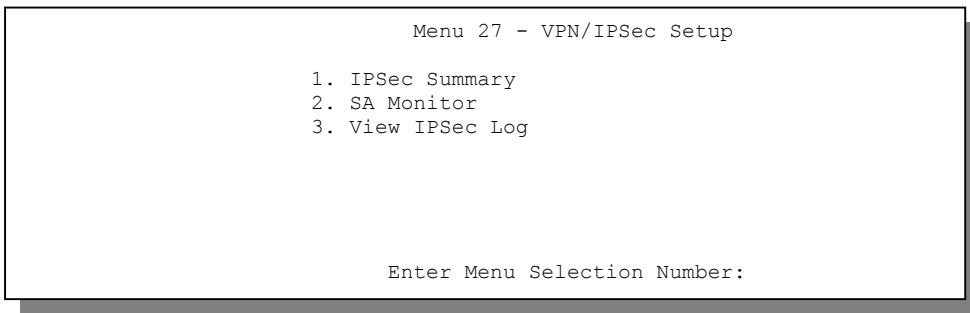


Figure 25-2 Menu 27 — VPN/IPSec Setup

25.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

25.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

25.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 25-1 AH and ESP

ESP	AH
Select DES for minimal security and 3DES for maximum. Select NULL to set up a tunnel without encryption.	Select MD5 for minimal security and SHA-1 for maximum security.
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

25.3 IPSec Summary

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

The following figure helps explain the main fields in menu 27.1.

Local Network

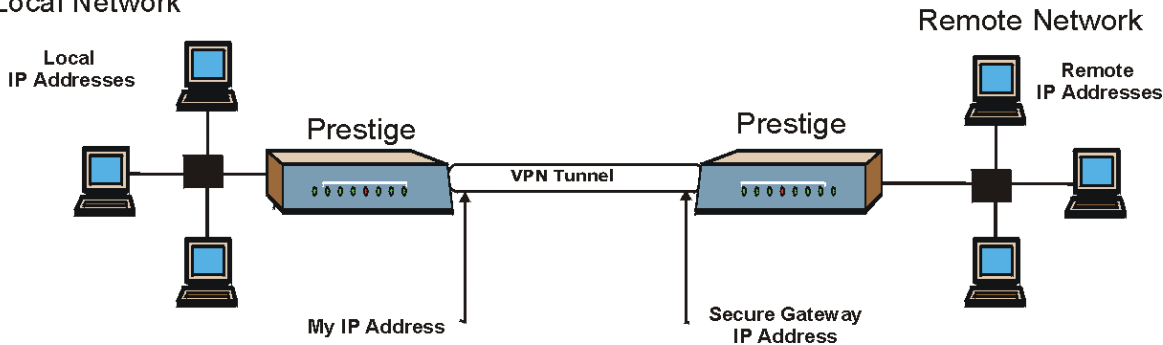


Figure 25-3 IPSec Summary Fields

Local and remote IP addresses must be static. The VPN initiator local IP address range should be identical to the peer remote IP address range. Similarly, the VPN initiator remote IP address range should be identical to the peer local IP address range. If they are not, the connection will fail and this will display in the IPSec log as a local or remote ID failure.

25.3.1 My IP Address

My IP Addr is the WAN IP address of the Prestige. If this field is configured as 0.0.0.0, then the Prestige will use the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel. If the **My IP Addr** changes after setup, then the VPN tunnel will have to be rebuilt.

25.3.2 Secure Gateway Address

Secure Gateway Addr is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static public IP address, enter it in the **Secure Gateway Addr** field.

You may alternatively enter the remote secure gateway's domain name in the **Secure Gateway Addr** field. This also works when the remote secure gateway uses DDNS. This way your Prestige can find the remote secure gateway, even if it has a dynamic WAN IP address.

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 in the **Secure Gateway Addr** field. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See the following table for an example configuration.

You can configure multiple SAs to simultaneously connect through the same secure gateway. In this case, you must configure the SAs to have the same **Negotiation Mode** and **Pre-Shared Key (Menu 27.1.1.1 IKE Setup)**.

Table 25-2 Telecommuter and Headquarters Configuration Example

	TELECOMMUTER	HEADQUARTERS
My IP address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address or domain name	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

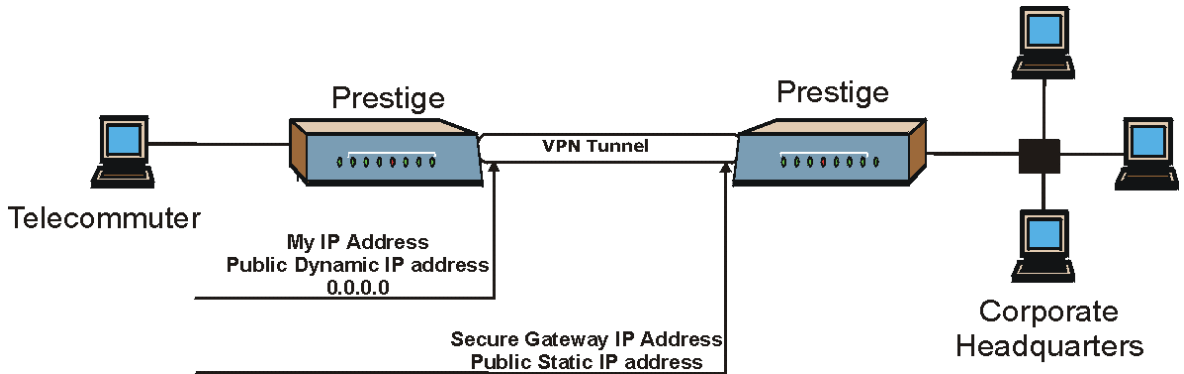


Figure 25-4 Telecommuter's Prestige Configuration

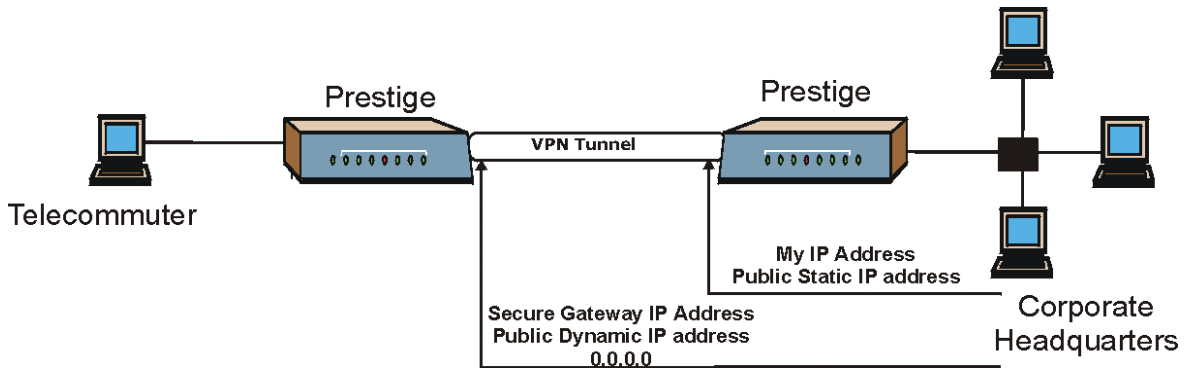


Figure 25-5 Headquarters Prestige Configuration

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using IKE key management and not Manual key management.

A Prestige with Secure Gateway Address set to 0.0.0.0 can receive multiple VPN connection requests using the same VPN rule at the same time.

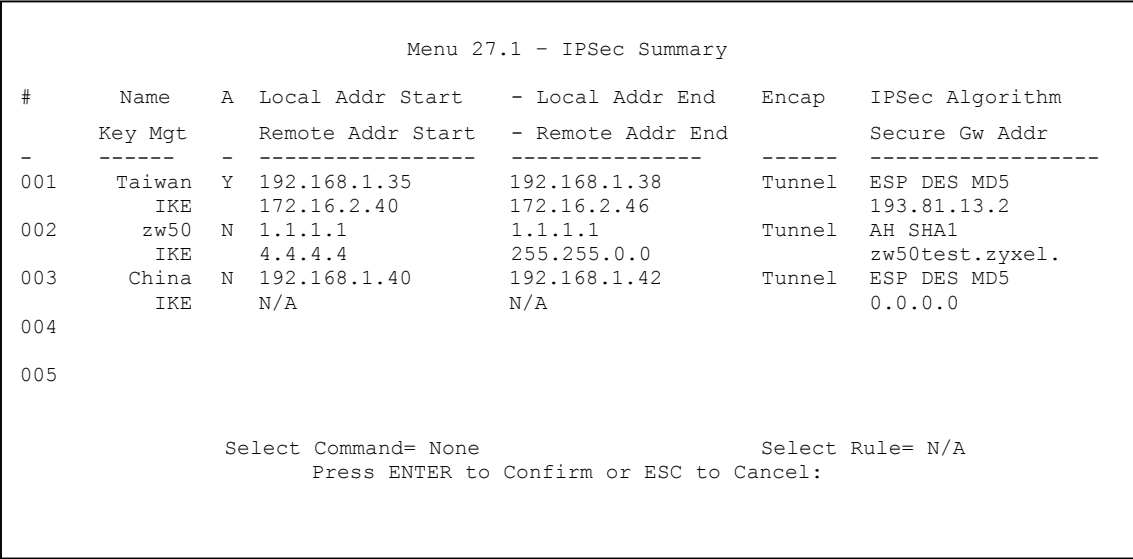


Figure 25-6 Menu 27.1 — IPSec Summary

Table 25-3 Menu 27.1 — IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	001
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.	Taiwan
A	Y signifies that this VPN rule is active.	Y
Local Addr Start	When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Single , this is a (static) IP address on the LAN behind your Prestige. When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Range , this is the beginning (static) IP address, in a range of computers on the LAN behind your Prestige. When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to SUBNET , this is a (static) IP address on the LAN behind your Prestige.	192.168.1.35
Local Addr End	When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Single , this is the same (static) IP address as in the Local Addr Start	192.168.1.38

Table 25-3 Menu 27.1 — IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
	<p>field.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Range, this is the end (static) IP address, in a range of computers on the LAN behind your Prestige.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to SUBNET, this is a subnet mask on the LAN behind your Prestige.</p>	
Encap	This field displays Tunnel mode or Transport mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if ??? is displayed.	Tunnel
IPSec Algorithm	<p>This field displays the security protocols used for an SA. ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit DES and 168-bit 3DES. NULL denotes a tunnel without encryption.</p> <p>AH (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. AH choices are MD5 (default - 128 bits) and SHA -1 (160 bits).</p> <p>Both AH and ESP increase the Prestige's processing requirements and communications latency (delay).</p> <p>You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if ??? is displayed.</p>	ESP DES MD5
Key Mgt	This field displays the SA's type of key management, (IKE or Manual).	IKE
Remote Addr Start	<p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Single, this is a (static) IP address on the network behind the remote IPSec router.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Range, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to SUBNET, this is a (static) IP address on the network behind the remote IPSec router.</p> <p>This field displays N/A when you configure the Secure Gateway Addr field in SMT 27.1.1 to 0.0.0.0.</p>	172.16.2.40

Table 25-3 Menu 27.1 — IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
Remote Addr End	<p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Single, this is the same (static) IP address as in the Remote Addr Start field.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to Range, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>When the Addr Type field in Menu 27.1.1 IPSec Setup is configured to SUBNET, this is a subnet mask on the network behind the remote IPSec router.</p> <p>This field displays N/A when you configure the Secure Gateway Addr field in SMT 27.1.1 to 0.0.0.0.</p>	172.16.2.46
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays 0.0.0.0 when you configure the Secure Gateway Addr field in SMT 27.1.1 to 0.0.0.0.	193.81.13.2
Select Command	<p>Press [SPACE BAR] to choose from None, Edit or Delete and then press [ENTER]. You must select a rule in the next field when you choose the Edit, Delete or Go To commands.</p> <p>Select None and then press [ENTER] to go to the “Press ENTER to Confirm...” prompt.</p> <p>Use Edit to create or edit a rule. Use Delete to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do <u>not</u> move up in the page list.</p>	None
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

25.4 IPSec Setup

Select **Edit** in the **Select Command** field, type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

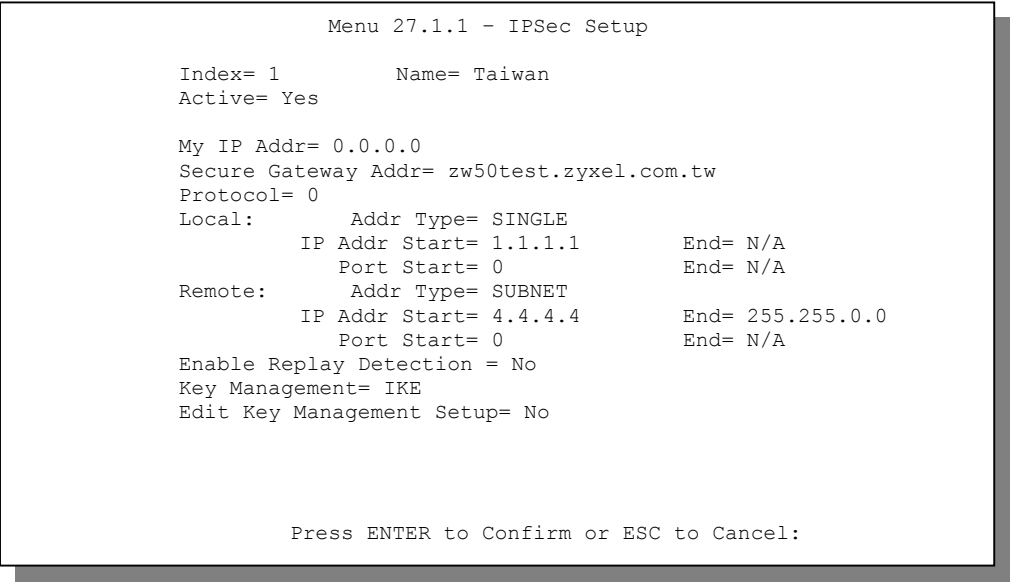


Figure 25-7 Menu 27.1.1 — IPSec Setup

You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

Table 25-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	1
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in Menu 27.1 - IPSec Summary .	Taiwan
Active	Press [SPACE BAR] to choose either Yes or No . Choose Yes and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.	Yes
My IP Addr	Enter the WAN IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0.	0.0.0.0

Table 25-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
	The VPN tunnel has to be rebuilt if this IP address changes.	
Secure Gateway Addr	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the Key Management field must be set to IKE , see later). See the <i>Secure Gateway Address</i> section for more details.	Zw50test.com. tw
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose SINGLE , RANGE , or SUBNET and press [ENTER]. Select SINGLE with a single IP address. Select RANGE for a specific range of IP addresses. Select SUBNET to specify IP addresses on a network by their subnet mask.	SINGLE
IP Addr Start	When the Addr Type field is configured to Single , enter a (static) IP address on the LAN behind your Prestige. When the Addr Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the Addr Type is configured to SUBNET , this is a (static) IP address on the LAN behind your Prestige.	192.168.1.35
End	When the Addr Type field is configured to Single , this field is N/A . When the Addr Type field is configured to Range , enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the Addr Type field is configured to SUBNET , this is a subnet mask on the LAN behind your Prestige.	192.168.1.38
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0

Table 25-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is N/A when 0 is configured in the Port Start field.	N/A
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are N/A when the Secure Gateway Addr field is configured to 0.0.0.0. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.	
Addr Type	Press [SPACE BAR] to choose SINGLE , RANGE , or SUBNET and press [ENTER]. Select SINGLE with a single IP address. Use RANGE for a specific range of IP addresses. Use SUBNET to specify IP addresses on a network by their subnet mask.	SUBNET
IP Addr Start	When the Addr Type field is configured to Single , enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to Range , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Addr Type field is configured to SUBNET , enter a (static) IP address on the network behind the remote IPSec router. This field displays N/A when you configure the Secure Gateway Addr field to 0.0.0.0.	4.4.4.4
End	When the Addr Type field is configured to Single , this field is N/A . When the Addr Type field is configured to Range , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the Addr Type field is configured to SUBNET , enter a subnet mask on the network behind the remote IPSec router. This field displays N/A when you configure the Secure Gateway Addr field to 0.0.0.0.	255.255.0.0
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.	0

Table 25-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is N/A when 0 is configured in the Port Start field.	
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to Yes . Press [SPACE BAR] to select Yes or No . Choose Yes and press [ENTER] to enable replay detection.	No
Key Management	Press [SPACE BAR] to choose either IKE or Manual and then press [ENTER]. Manual is useful for troubleshooting if you have problems using IKE key management.	IKE
Edit Key Management Setup	Press [SPACE BAR] to change the default No to Yes and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the Key Management field to IKE , this will take you to Menu 27.1.1.1 – IKE Setup . If you set the Key Management field to Manual , this will take you to Menu 27.1.1.2 – Manual Setup .	No
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

25.5 IKE Setup

To edit this menu, the **Key Management** field **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

25.5.1 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

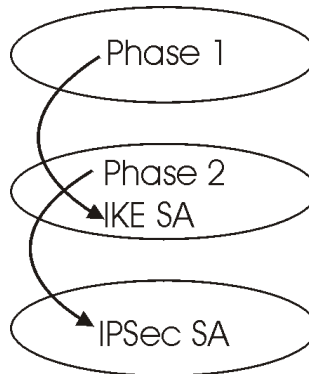


Figure 25-8 Two Phases to set up the IPsec SA

In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long IKE SA negotiation should proceed before it times out. A value of **0** means IKE SA negotiation never times out. If IKE SA negotiation times out, then both IKE SA and IPsec SA must be renegotiated.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 25.5.5*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPsec SA lifetime. This field allows you to determine how long IPsec SA setup should proceed before it times out. A value of **0** means IPsec SA never times out. If IPsec SA negotiation times out, then the IPsec SA must be renegotiated (but not the IKE SA).

25.5.2 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips (SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number)). This mode features identity protection (your identity is not revealed in the negotiation).

- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

25.5.3 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

25.5.4 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

25.5.5 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPsec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Prestige. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

```
Menu 27.1.1.1 - IKE Setup

Phase 1
Negotiation Mode= Main
Pre-Shared Key= ?
Encryption Algorithm = DES
Authentication Algorithm = MD5
SA Life Time (Seconds)= 28800
Key Group= DH1

Phase 2
Active Protocol = ESP
Encryption Algorithm = DES
Authentication Algorithm = SHA1
SA Life Time (Seconds)= 28800
Encapsulation = Tunnel
Perfect Forward Secrecy (PFS)= None

Press ENTER to Confirm or ESC to Cancel:
```

Figure 25-9 Menu 27.1.1.1 — IKE Setup

Table 25-5 Menu 27.1.1.1 — IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Phase 1		
Negotiation Mode	Press [SPACE BAR] to choose from Main or Aggressive and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.	Main
Pre-Shared Key	Prestige gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key.	
Encryption Algorithm	When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Prestige DES encryption algorithm uses a 56-bit key. Triple DES (3DES), is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES . It also requires more processing power, resulting in slightly increased latency and decreased throughput.	DES

Table 25-5 Menu 27.1.1.1 — IKE Setup

FIELD	DESCRIPTION	EXAMPLE
	Press [SPACE BAR] to choose from 3DES or DES and then press [ENTER].	
Authentication Algorithm	MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slightly slower. Press [SPACE BAR] to choose from SHA1 or MD5 and then press [ENTER].	MD5
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.	28800 (default)
Key Group	You must choose a key group for phase 1 IKE setup. DH1 (default) refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.	DH1
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from ESP or AH and then press [ENTER]. See earlier for a discussion of these protocols.	ESP
Encryption Algorithm	Press [SPACE BAR] to choose from NULL , 3DES or DES and then press [ENTER]. Select NULL to set up a tunnel without encryption.	DES
Authentication Algorithm	Press [SPACE BAR] to choose from SHA1 or MD5 and then press [ENTER].	SHA1
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).	28800 (default)
Encapsulation	Press [SPACE BAR] to choose from Tunnel mode or Transport mode and then press [ENTER]. See earlier for a discussion of these.	Tunnel
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Press [SPACE BAR] and choose from DH1 or DH2 to enable PFS. DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).	None
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

25.6 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPsec Setup**. Manual key management is useful if you have problems with **IKE** key management.

25.6.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. These parameters have been discussed earlier.

Table 25-6 Active Protocol — Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

25.6.2 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPsec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPsec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

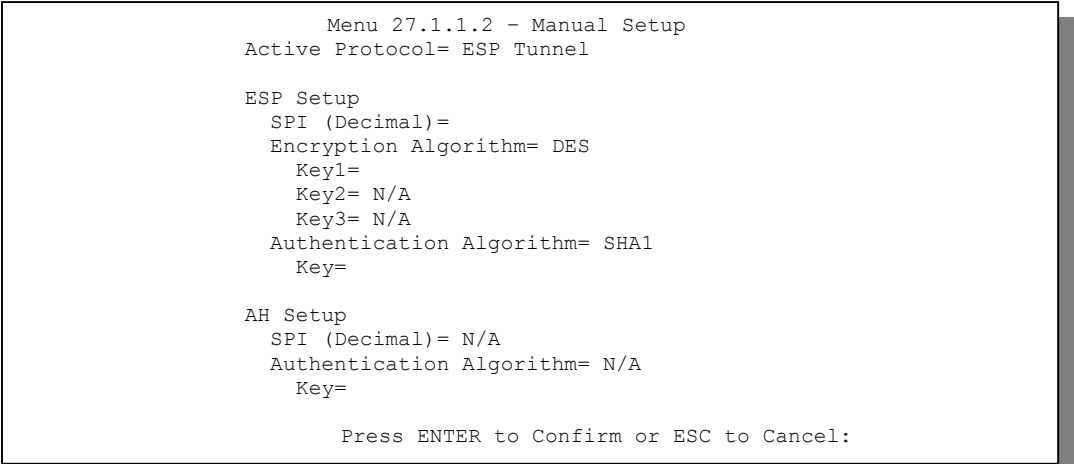


Figure 25-10 Menu 27.1.1.2 — Manual Setup

Table 25-7 Menu 27.1.1.2 — Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from ESP Tunnel , ESP Transport , AH Tunnel or AH Transport and then press [ENTER]. Choosing an ESP combination causes the AH Setup fields to be non-applicable (N/A)	ESP Tunnel
ESP Setup	The ESP Setup fields are N/A if you chose an AH Active Protocol .	
SPI (Decimal)	The SPI must be unique and from one to four integers ("0" to "9").	1234
Encryption Algorithm	Press [SPACE BAR] to choose from NULL , 3DES or DES and then press [ENTER]. Fill in the Key1 field below when you choose DES and fill in fields Key1 to Key3 when you choose 3DES . Select NULL to set up a tunnel without encryption. When you select NULL , you do not enter any encryption keys.	DES
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the Key1 field when you choose DES and fill in fields Key1 to Key3 when you choose 3DES .	89abcde
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).	

Table 25-7 Menu 27.1.1.2 — Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Authentication Algorithm	Press [SPACE BAR] to choose from MD5 or SHA1 and then press [ENTER].	SHA1
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for MD5 authentication and 20 characters for SHA-1 authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789abcde
AH Setup	The AH Setup fields are N/A if you chose an ESP Active Protocol .	
SPI (Decimal)	The SPI must be from one to four unique decimal characters ("0" to "9") long.	N/A
Authentication Algorithm	Press [SPACE BAR] to choose from MD5 or SHA1 and then press [ENTER].	N/A
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for MD5 authentication and 20 characters for SHA-1 authentication. Any character may be used, including spaces, but trailing spaces are truncated.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Chapter 26

SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

1.1. Introduction

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

An SA times out automatically after one minute if there is no traffic.

- 1. Use the **Refresh** function to display active VPN connections.
- 2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

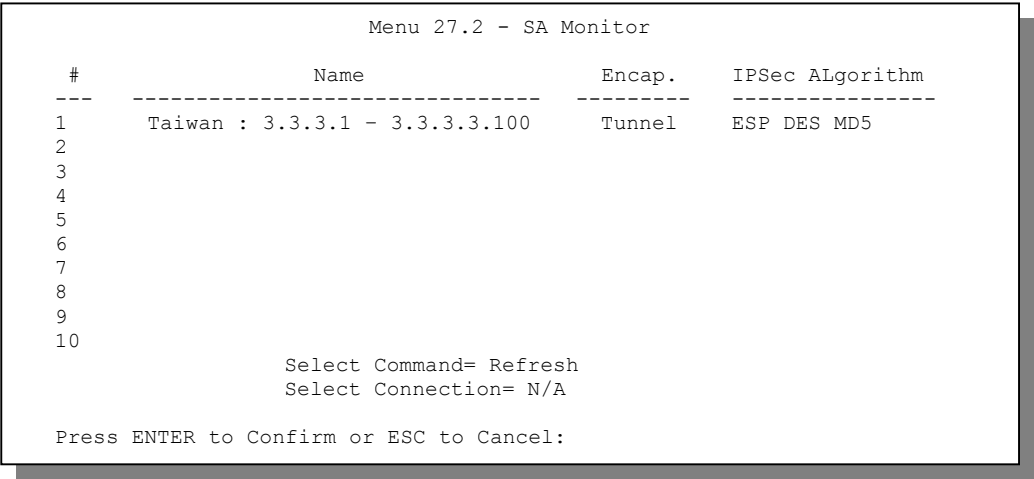


Figure 26-1 Menu 27.2 — SA Monitor

Table 26-1 Menu 27.2 — SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	1
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a	Taiwan

Table 26-1 Menu 27.2 — SA Monitor

FIELD	DESCRIPTION	EXAMPLE
	<p>public static IP address.</p> <p>When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in Menu 27.1.1. – IPSec Setup. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.</p>	
Encap.	This field displays Tunnel mode or Transport mode. See previous for discussion.	Tunnel
IPSec Algorithm	<p>This field displays the security protocols used for an SA. ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit DES and 168-bit 3DES. NULL denotes a tunnel without encryption.</p> <p>An incoming SA may have an AH in addition to ESP. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. AH choices are MD5 (default - 128 bits) and SHA -1(160 bits).</p> <p>Both AH and ESP increase Prestige processing requirements and communications latency (delay).</p>	ESP DES MD5
Select Command	Press [SPACE BAR] to choose from Refresh , Disconnect or None and then press [ENTER]. You must select a connection in the next field when you choose the Disconnect command. Refresh displays current active VPN connections. None allows you to jump to the “Press ENTER to Confirm...” prompt.	Refresh
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	1
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 27

IPSec Log

This chapter interprets common IPSec log messages.

27.1 IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

Index:	Date/Time:	Log:

001	01 Jan 08:02:22	Send Main Mode request to <192.168.100.101>
002	01 Jan 08:02:22	Send:<SA>
003	01 Jan 08:02:22	Recv:<SA>
004	01 Jan 08:02:24	Send:<KE><NONCE>
005	01 Jan 08:02:24	Recv:<KE><NONCE>
006	01 Jan 08:02:26	Send:<ID><HASH>
007	01 Jan 08:02:26	Recv:<ID><HASH>
008	01 Jan 08:02:26	Phase 1 IKE SA process done
009	01 Jan 08:02:26	Start Phase 2: Quick Mode
010	01 Jan 08:02:26	Send:<HASH><SA><NONCE><ID><ID>
011	01 Jan 08:02:26	Recv:<HASH><SA><NONCE><ID><ID>
012	01 Jan 08:02:26	Send:<HASH>
Clear IPSec Log (y/n):		

Figure 27-1 Example VPN Initiator IPSec Log

The following figure shows a typical log from the VPN connection peer.

Index:	Date/Time:	Log:
001	01 Jan 08:08:07	Recv Main Mode request from <192.168.100.100>
002	01 Jan 08:08:07	Recv:<SA>
003	01 Jan 08:08:08	Send:<SA>
004	01 Jan 08:08:08	Recv:<KE><NONCE>
005	01 Jan 08:08:10	Send:<KE><NONCE>
006	01 Jan 08:08:10	Recv:<ID><HASH>
007	01 Jan 08:08:10	Send:<ID><HASH>
008	01 Jan 08:08:10	Phase 1 IKE SA process done
009	01 Jan 08:08:10	Recv:<HASH><SA><NONCE><ID><ID>
010	01 Jan 08:08:10	Start Phase 2: Quick Mode
011	01 Jan 08:08:10	Send:<HASH><SA><NONCE><ID><ID>
012	01 Jan 08:08:10	Recv:<HASH>
Clear IPSec Log (y/n):		

Figure 27-2 Example VPN Responder IPSec Log

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Table 27-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Cannot find outbound SA for rule <#d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
Send Main Mode request to <IP> Send Aggressive Mode request to <IP>	The Prestige has started negotiation with the peer.
Recv Main Mode request from <IP> Recv Aggressive Mode request from <IP>	The Prestige has received an IKE negotiation request from the peer.
Send:<Symbol><Symbol> Recv:<Symbol><Symbol>	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see <i>Table 27-3</i> .
Phase 1 IKE SA process done	Phase 1 negotiation is finished.

Table 27-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.
!! IKE Negotiation is in process	The Prestige has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
!! Duplicate requests with the same cookie	The Prestige has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
!! Verifying Local ID failed !! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the Prestige will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the Prestige will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The Prestige limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The Prestige did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The Prestige cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The Prestige deletes an SA when too many errors occur.

The following table shows sample log messages during packet transmission.

Table 27-2 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the Prestige's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0".. If this field is configured as 0.0.0.0, then the Prestige will use the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 SA	The Prestige cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Discard REPLAY packet	If the Prestige receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the Prestige drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 27-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature

Table 27-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Chapter 28

Internal SPTGEN

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual SMT menus for each Prestige.

28.1 The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values allowed =  
input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

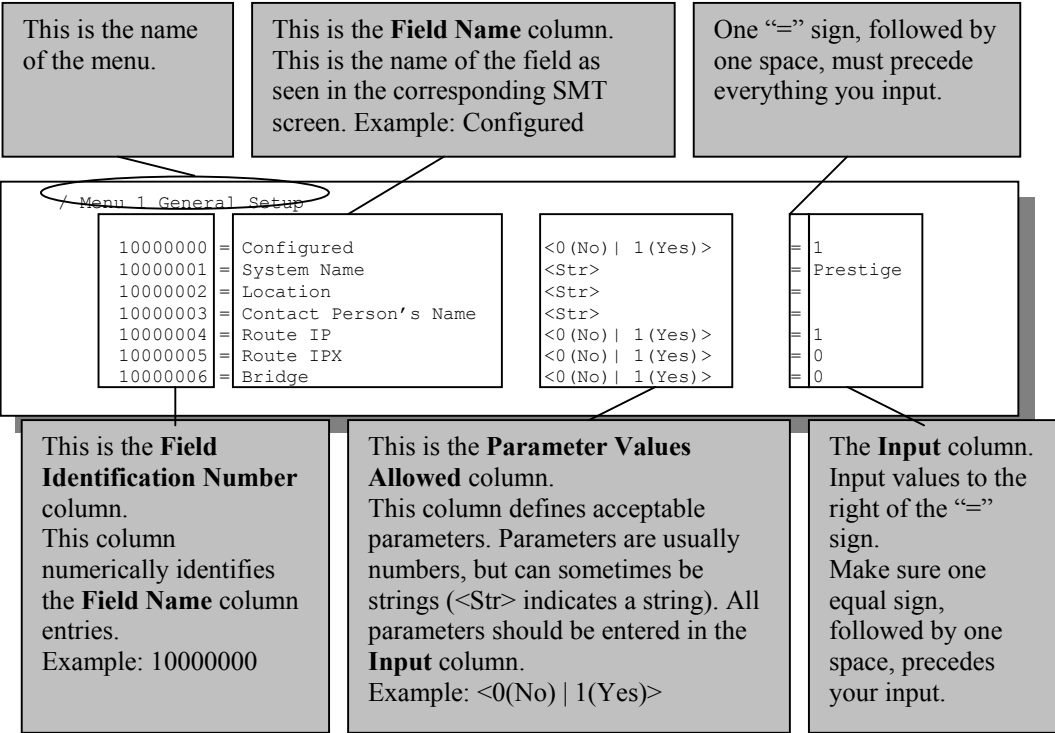


Figure 28-1 Configuration Text File Format — Column Descriptions

DO NOT alter or delete any field except parameters in the Input column.

For more text file examples, refer to the *Example Internal SPTGEN Screens Appendix*.

28.1.1 Internal SPTGEN File Modification - Important Points to Remember

- Each parameter you enter must be preceded by one “=” sign and one space.
- Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see *Figure 28-1*), then you disable every field in this menu.
- If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. *Figure 28-2*, shown next, is an example of what the Prestige displays if you enter a value other than “0” or “1” in the **Input** column of **Field Identification Number** 1000000 (refer to *Figure 28-1*).

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Figure 28-2 Invalid Parameter Entered — Command Line Example

The Prestige will display the following if you enter parameter(s) that *are* valid.

```
Please wait for the system to write SPT text file(ROM-
t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Figure 28-3 Valid Parameter Entered — Command Line Example

28.2 Internal SPTGEN FTP Download Example

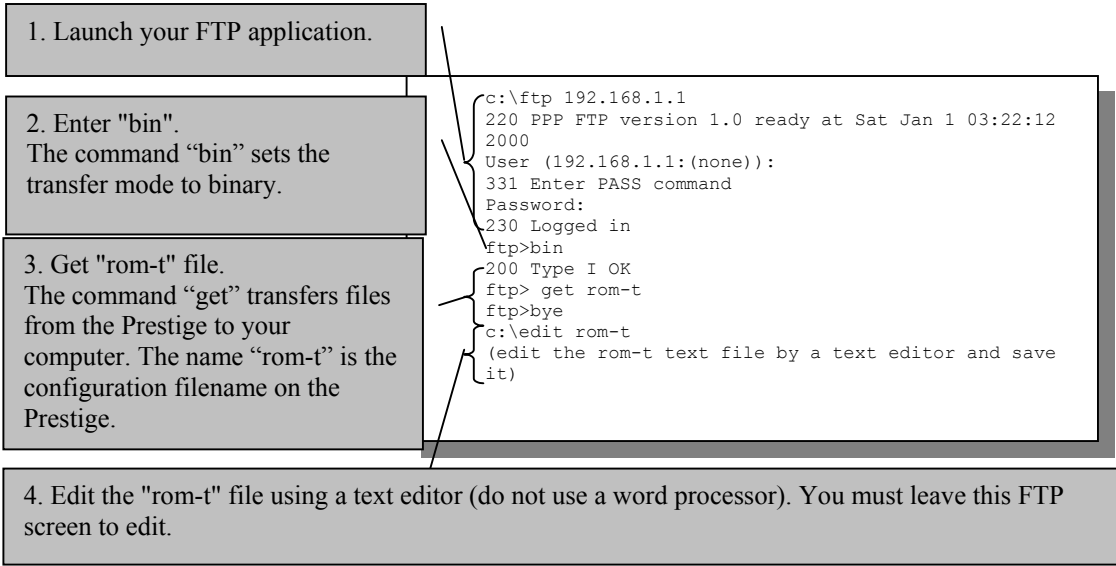


Figure 28-4 Internal SPTGEN FTP Download Example

You can rename your “rom-t” file when you save it to your computer but it must be named “rom-t” when you upload it to your Prestige.

28.3 Internal SPTGEN FTP Upload Example

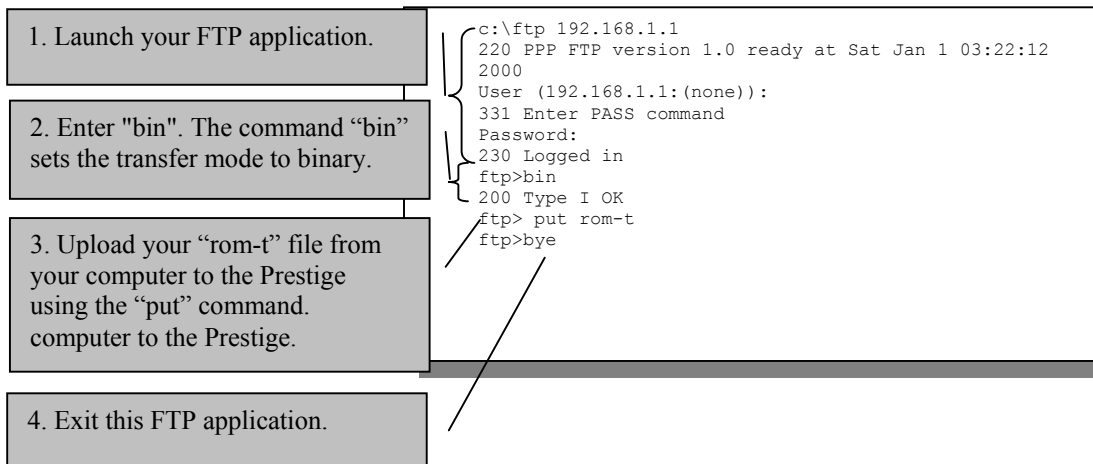


Figure 28-5 Internal SPTGEN FTP Upload Example

Part:VI

ADDITIONAL INFORMATION

This part contains Troubleshooting, Appendices and the Index.

Chapter 29

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

29.1 Problems Starting Up the Prestige

Table 16-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adapter is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. Turn the Prestige off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
I cannot access the Prestige via the console port.	1. Make sure the Prestige is connected to your computer's serial port.	
	2. Make sure the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation.
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

29.2 Problems with the LAN LED

Table 29-1 Troubleshooting the LAN LED

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections and type (crossover when connecting to a computer or straight-through when connecting to a hub).
	Check for faulty Ethernet cables.
	Make sure your computer NIC (Network Interface Card) is working properly.

29.3 Problems with the DSL LED

Table 29-2 Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The xDSL LED is off.	Check the telephone wire and connections between the Prestige DSL port and the wall jack.
	Make sure that the telephone company has checked your phoneline and set it up for DSL service.
	Reset your xDSL line in SMT menu 24.4 to reinitialize your link to the DSLAM.

29.4 Problems with the LAN Interface

Table 29-3 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the <i>Problems with the LAN LED</i> section. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the <i>Problems with the LAN LED</i> section. Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

29.5 Problems with the WAN Interface

Table 29-4 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP is provided after the ISP verifies the MAC address, host name or user ID. Find out the verification method used by your ISP and configure the corresponding fields.

29.6 Problems with Internet Access

Table 29-5 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. If the DSL LED is off, refer to the <i>Problems with the DSL LED</i> section. Verify your settings in SMT menus 3.2 and 4. Make sure you use correct casing when typing entries.
Internet connection disconnects.	Check the schedule rules in SMT menu 26. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in SMT menu 11.1. Contact your ISP.

29.7 Problems with the Password

Table 29-6 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The default password is “1234”. The Password field is case-sensitive. If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to the <i>Resetting the Prestige</i> section). This restores all of the factory defaults including the password.

29.8 Problems with the Web Configurator

Table 29-7 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	<p>Type “admin” in the User Name field. The default password is “1234”. Both fields are case-sensitive.</p> <p>If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to the <i>Resetting the Prestige</i> section). This restores all of the factory defaults including the password.</p> <p>Make sure that there is not an SMT console session running.</p> <p>Check that you have enabled web service access in SMT Menu 24.11 - Remote Management Control. If you have configured an IP address in the Secured Client IP field, your computer's IP address must match it. For WAN access, you must configure the Server Access field to WAN only or ALL. Otherwise, the firewall (when activated) blocks all WAN to LAN traffic by default.</p> <p>Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the Prestige's LAN IP address, then enter the new one as the URL.</p> <p>Remove any filters in menu 3.1 (LAN) or menu 11.5 (WAN) that block web service.</p>

29.9 Problems with Remote Management

Table 29-8 Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
I cannot remotely manage the Prestige from the LAN or WAN.	Refer to the <i>Remote Management Limitations</i> section for scenarios when remote management may not be possible.
	When NAT is enabled: <ul style="list-style-type: none">➤ Use the Prestige's WAN IP address when configuring from the WAN.➤ Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to the <i>Problems with the LAN Interface</i> section for instructions on checking your LAN connection.
	Refer to the <i>Problems with the WAN Interface</i> section for instructions on checking your WAN connection.

Appendix A

PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

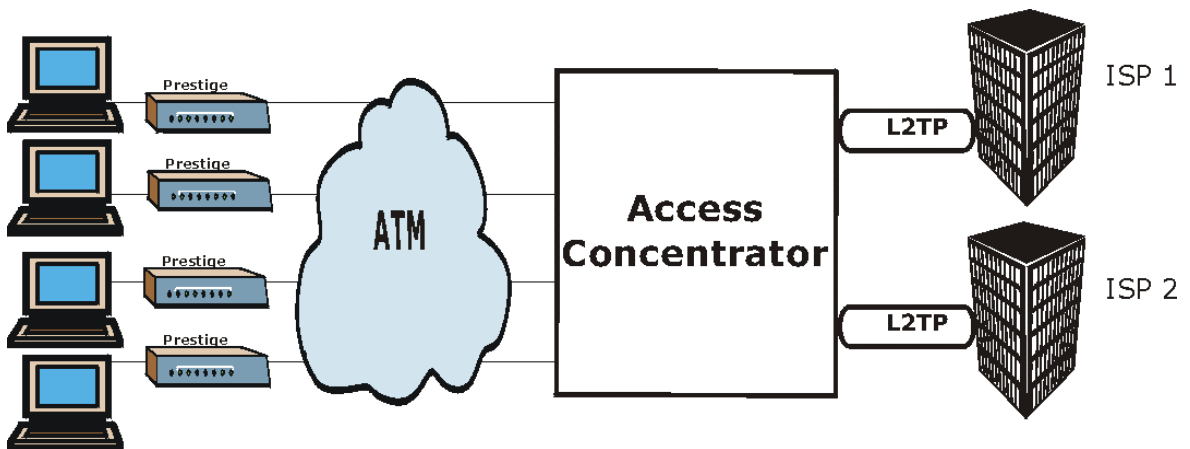


Diagram 1 Single-PC per Router Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

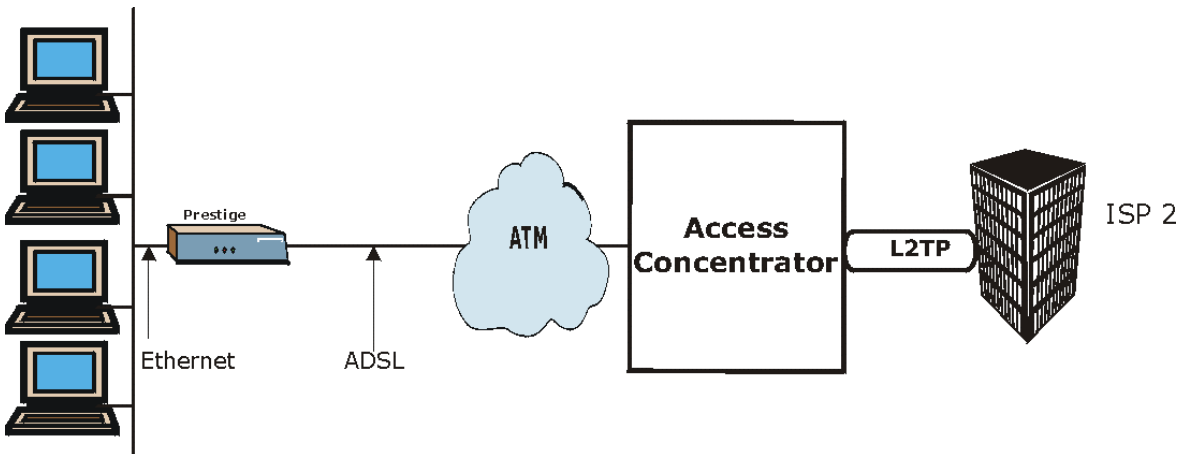


Diagram 2 Prestige as a PPPoE Client

Appendix B

Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel Logical connections between ATM switches
- Virtual Path A bundle of virtual channels
- Virtual Circuit A series of virtual paths between circuit end points

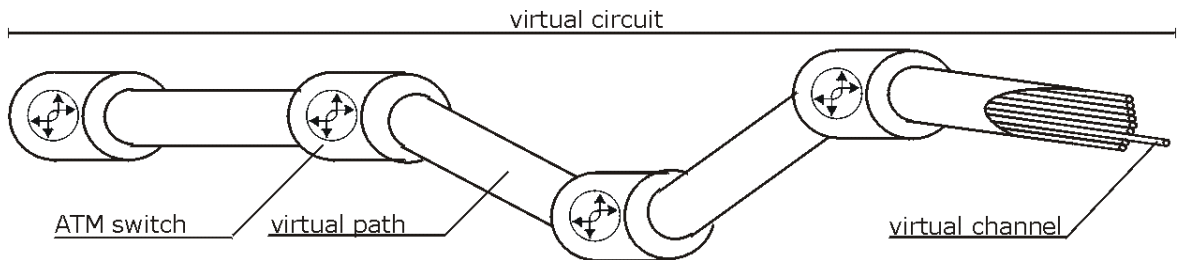


Diagram 3 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix C

Boot Module Commands

When you reboot your Prestige, you will be given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file) already discussed in a previous section.

```
Bootbase Version: V1.02 | 10/11/2001 13:36:19
RAM: Size = 8192 Kbytes
DRAM POST: Testing: 8192K
OK
FLASH: Intel 16M *1

ZyNOS Version: V3.40(ES.0)b8 | 12/4/2001 12:54:08

Press any key to enter debug mode within 3 seconds.
.....
```

Diagram 4 Option to Enter Debug Mode

Type "ATHE" to view all available Prestige boot module commands. Some are shown in the next screen. Most commands aid in advanced troubleshooting and should only be used by qualified engineers.

```
===== Debug Command Listing =====
AT          just answer OK
ATHE        print help
ATBAX       change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)   set BootExtension Debug Flag (y=password)
ATSE        show the seed of password generator
ATTI(h,m,s) change system time to hour:min:sec or show current time
ATDA(y,m,d) change system date to year/month/day or show current date
ATDS        dump RAS stack
ATDT        dump Boot Module Common Area
ATDUX,y     dump memory contents from address x for length y
ATRBx       display the 8-bit value of address x
ATRWx       display the 16-bit value of address x
ATRLx       display the 32-bit value of address x
ATGO(x)     run program at addr x or boot router
ATGR        boot router
ATGT        run Hardware Test Program
ATRTw,x,y,(z) RAM test level w, from address x to y (z iterations)
ATSH        dump manufacturer related data in ROM
ATDOx,y     download from address x for length y to PC via XMODEM
ATTD        download router configuration to PC via XMODEM
ATUR        upload router firmware to flash ROM
ATLC        upload router configuration file to flash ROM
ATXSx       xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSS        display system registers
```

Diagram 5 Boot Module Commands

Appendix D

Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-1215A
Input Power	AC120Volts/60Hz/30W
Output Power	AC12Volts/1.25A
Power Consumption	11 W
Safety Standards	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A25
Input Power	AC120Volts/60Hz/19W
Output Power	AC12Volts/1.25A
Power Consumption	11 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A3BN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	11 W
Safety Standards	TUV, CE (EN 60950)

Appendix E

TCP/IP

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Setting up Your Windows 95/98/Me Computer

Installing TCP/IP Components

1. Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon.

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

- a. Click **Add**.

- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

Configuring TCP/IP

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.
2. Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.
3. Click the **DNS Configuration** tab.
 - If you do not know your DNS information, select **Disable DNS**.
 - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).
4. Click the **Gateway** tab.
 - If you do not know your gateway's IP address, remove previously installed gateways.
 - If you have a gateway IP address, type it in the **New gateway** field and click **Add**.
5. Click **OK** to save and close the **TCP/IP Properties** window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying TCP/IP Properties

1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Setting up Your Windows NT/2000 Computer

Configuring TCP/IP

1. Click **Start, Settings, Network** and **Dial-up Connections** and right-click **Local Area Connection** or the connection you want to configure and click **Properties**.
2. Select **Internet Protocol (TCP/IP)** (you may need to scroll down) and click **Properties**.
3. The **Internet Protocol TCP/IP Properties** window opens.
 - If your IP address is dynamic, click **Obtain an IP address automatically**.
 - If you have a static IP address click Use the following IP Address and fill in the **IP address, Subnet mask, and Default gateway** fields.
4. In the **Internet Protocol TCP/IP Properties** window:
 - Click **Obtain DNS server automatically** if you do not know your DNS server IP address(es).
 - If you know your DNS server IP address(es), type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS tab** to order them.
5. Click **Advanced**:
 - If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.
6. Click **OK** to save and close the **Internet Protocol (TCP/IP) Properties** window.
7. Click **OK** to close the **Local Area Connection Properties** window.
8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Click **Start, Programs, Accessories** and then **Command Prompt**.

In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. The window will display information about your connection-specific DNS suffix, IP Address, Subnet Mask and Default Gateway.

Setting up Your Windows XP Computer

Configuring TCP/IP

1. Click **start, Control Panel, Network and Internet Connections** and then **Network Connections**.
2. Right-click the network connection you want to configure and then click **Properties**.
3. Under the **General** tab, select Internet Protocol (TCP/IP) (you may need to scroll down) and click **Properties**.
4. The **Internet Protocol TCP/IP Properties** window opens.
 - If you have a dynamic IP address click **Obtain an IP address automatically**.

-If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. To configure advanced static address settings for a local area connection, click **Advanced**, and do one or more of the following to configure additional IP addresses:

-In the **IP Settings** tab, in **IP addresses**, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

5. In the **Internet Protocol TCP/IP Properties** window's **General** tab:

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click **Use the following DNS server addresses**, type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

6. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

7. Click **OK** to close the **Local Area Connection Properties** window.

8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Setting up Your Macintosh Computer

Configuring TCP/IP Properties

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

2. Select **Ethernet** from the **Connect via** list.

3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Check your TCP/IP properties in the **TCP/IP Control Panel**.

Appendix F

Example Internal SPTGEN Screens

This appendix covers Prestige Internal SPTGEN screens.

Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name
PVA	Parameter Values Allowed
INPUT	This is an example of what you may enter

The following are Internal SPTGEN screens associated with the SMT screens of your Prestige.

Example Internal SPTGEN Screens Table

/ MENU 1 GENERAL SETUP (SMT MENU 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0(No) 1(Yes)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(No) 1(Yes)>	= 1
10000006 =	Bridge	<0(No) 1(Yes)>	= 0

/ MENU 3.1 GENERAL ETHERNET SETUP (SMT MENU 3.1)			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ MENU 3.2 TCP/IP AND DHCP ETHERNET SETUP (SMT MENU 3.2)			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(None) 1(Server) 2(Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0

The valid parameters for a set are 1-12. Type "256" if you do not want to select a set.

This value must be between 1-254.

30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0(None) 1(Both) 2(In Only) 3(Out Only)>	= 0
30200011 =	Version	<0(Rip-1) 1(Rip-2B) 2(Rip-2M)>	= 0
30200012 =	Multicast	<0(IGMP-v2) 1(IGMP-v1) 2(None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ MENU 3.2.1 IP ALIAS SETUP (SMT MENU 3.2.1)			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0(No) 1(Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0(None) 1(Both) 2(In Only) 3(Out Only)>	= 0
30201005 =	Version	<0(Rip-1) 1(Rip-2B) 2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256

This value must be between 0-32.

This value must be between 0-32.

30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0(No) 1(Yes)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0
30201017 =	RIP Direction	<0(None) 1(Both) 2(In Only) 3(Out Only)>	= 0
30201018 =	Version	<0(Rip-1) 1(Rip-2B) 2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256

/ MENU 4 INTERNET ACCESS SETUP (SMT MENU 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0(No) 1(Yes)>	= 1
40000001 =	ISP	<0(No) 1(Yes)>	= 1
40000002 =	Active	<0(No) 1(Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) 3(RFC 1483) 4(PPPoA) 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1(LLC-based) 2(VC-based)>	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@p
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0(No) 1(Yes)>	= 1
40000012 =	IP Address Assignment	<0(Static) 1(Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask	This value must be between 0-32.	= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256

This value must be between 0-32.

This value must be between 0-655355.

40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(No) 1(Yes)>	= 1
40000026 =	Bridge	<0(No) 1(Yes)>	= 0
40000027 =	ATM QoS Type	<0(CBR) 1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size(MBS)		= 0
/ MENU 12.1.1 IP STATIC ROUTE SETUP (SMT MENU 12.1.1)			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(No) 1(Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.2 IP STATIC ROUTE SETUP (SMT MENU 12.1.2)			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(No) 1(Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask	<div>This value must be between 0-8.</div>	<div>= 0</div>
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		<div>= 0</div>
120102007 =	IP Static Route set #2, Private	<0(No) 1(Yes)>	= 0

/ MENU 12.1.3 IP STATIC ROUTE SETUP (SMT MENU 12.1.3)			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0(No) 1(Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.4 IP STATIC ROUTE SETUP (SMT MENU 12.1.4)			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(No) 1(Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.5 IP STATIC ROUTE SETUP (SMT MENU 12.1.5)			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(No) 1(Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0

120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.6 IP STATIC ROUTE SETUP (SMT MENU 12.1.6)			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(No) 1(Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.7 IP STATIC ROUTE SETUP (SMT MENU 12.1.7)			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(No) 1(Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) 1(Yes)>	= 0
/ MENU 12.1.8 IP STATIC ROUTE SETUP (SMT MENU 12.1.8)			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No) 1(Yes)>	= 0

120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No) 1(Yes)>	= 0
/ MENU 15 SUA SERVER SETUP (SMT MENU 15)			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Port Start		= 0
150000003 =	SUA Server #2 Port End		= 0
150000004 =	SUA Server #2 Local IP Address		= 0.0.0.0
150000005 =	SUA Server #3 Port Start		= 0
150000006 =	SUA Server #3 Port End		= 0
150000007 =	SUA Server #3 Local IP address		= 0.0.0.0
150000008 =	SUA Server #4 Port Start		= 0
150000009 =	SUA Server #4 Port End		= 0
150000010 =	SUA Server #4 Local IP address		= 0.0.0.0
150000011 =	SUA Server #5 Port Start		= 0
150000012 =	SUA Server #5 Port End		= 0
150000013 =	SUA Server #5 Local IP address		= 0.0.0.0
150000014 =	SUA Server #6 Port Start		= 0
150000015 =	SUA Server #6 Port End		= 0
150000016 =	SUA Server #6 Local IP address		= 0.0.0.0
150000017 =	SUA Server #7 Port Start		= 0
150000018 =	SUA Server #7 Port End		= 0
150000019 =	SUA Server #7 Local IP address		= 0.0.0.0

150000020 =	SUA Server #8 Port Start		= 0	
150000021 =	SUA Server #8 Port End		= 0	
150000022 =	SUA Server #8 Local IP address		= 0.0.0.0	
150000023 =	SUA Server #9 Port Start		= 0	
150000024 =	SUA Server #9 Port End		= 0	
150000025 =	SUA Server #9 Local IP address		= 0.0.0.0	
150000026 =	SUA Server #10 Port Start		= 0	
150000027 =	SUA Server #10 Port End		= 0	
150000028 =	SUA Server #10 Local IP address		= 0.0.0.0	
150000029 =	SUA Server #11 Port Start		= 0	
150000030 =	SUA Server #11 Port End		= 0	
150000031 =	SUA Server #11 Local IP address		= 0.0.0.0	
150000032 =	SUA Server #12 Port Start		= 0	
150000033 =	SUA Server #12 Port End		= 0	
150000034 =	SUA Server #12 Local IP address		= 0.0.0.0	
/ MENU 21 FILTER SET #1 (SMT MENU 21)				
FIN	FN	PVA	INPUT	You may configure up to 12 filter sets with SMT menus; one with Internal SPTGEN.
210100001 =	Filter Set 1, Name	<Str>	=	
/ MENU 21.1.1 FILTER SET #1, RULE #1 (SMT MENU 21.1.1)				You may change this type using SMT menus only.
FIN	FN	PVA	INPUT	
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	=2	
210101002 =	IP Filter Set 1,Rule 1 Active	<0(No) 1(Yes)>	= 1	
210101003 =	IP Filter Set 1,Rule 1 Protocol	This value must be between 0-255.	= 6	
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0	
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0	
210101006 =	IP Filter Set 1,Rule 1 Dest Port	This value must be between 0-65535.	= 137	

210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(check next) 2(forward) 3(drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(check next) 2(forward) 3(drop)>	= 1
/ MENU 21.1.2 SET #1, RULE #2 (SMT MENU 21.1.2)			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(No) 1(Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0

210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1(check next) 2(forward) 3(drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1(check next) 2(forward) 3(drop)>	= 1
/ MENU 21.1.3 SET #1, RULE #3 (SMT MENU 21.1.3)			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0(No) 1(Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(check next) 2(forward) 3(drop)>	= 3

210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(check next) 2(forward) 3(drop)	= 1
/ MENU 21.1.4 SET #1, RULE #4 (SMT MENU 21.1.4)			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(No) 1(Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(check next) 2(forward) 3(drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(check next) 2(forward) 3(drop)	= 1
/ MENU 21.1.5 SET #1, RULE #5 (SMT MENU 21.1.5)			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0(No) 1(Yes)>	= 1

210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(check next) 2(forward) 3(drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1(Check Next) 2(Forward) 3(Drop)>	= 1
/ MENU 21.1.6 SET #1, RULE #6 (SMT MENU 21.1.6)			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(No) 1(Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139

210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(none) 1(equal) 2(not equal) 3(less) 4(greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(check next) 2(forward) 3(drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(check next) 2(forward) 3(drop)>	= 2

/ MENU 24.11 REMOTE MANAGEMENT CONTROL (SMT MENU 24.11)				
FIN	FN	PVA	INPUT	
241100001 =	TELNET Server Port		= 23	These values must be between 0-65535.
241100002 =	TELNET Server Access	<0(all) 1(none) 2(Lan) 3(Wan)>	= 0	
241100003 =	TELNET Server Secured IP address		= 0.0.0.0	
241100004 =	FTP Server Port		= 21	This value must be between 0-65535.
241100005 =	FTP Server Access	<0(all) 1(none) 2(Lan) 3(Wan)>	= 0	
241100006 =	FTP Server Secured IP address		= 0.0.0.0	
241100007 =	WEB Server Port		= 80	
241100008 =	WEB Server Access	<0(all) 1(none) 2(Lan) 3(Wan)>	= 0	
241100009 =	WEB Server Secured IP address		= 0.0.0.0	

Index

A	
Action for Matched Packets	12-11
ADSL Over ISDN	2-6
ADSL, what is it?	xxvii
Alert Schedule	11-4
Application-level Firewalls	9-1
AT command	19-1
Attack	
Reasons	14-2
Attack Alert	11-6, 11-8
Attack Types	9-6
Reason	10-3
Authentication	5-5, 5-6
auto-negotiation	1-3
B	
Back Panel	
Connections Description	2-3
Backup	19-2
Blocking Time	11-7, 11-8, 11-10
Bridging	3-5
Ether Address	7-3
Ethernet	7-1
Ethernet Addr Timeout	7-2
Remote Node	7-1
Static Route Setup	7-2
Brute-force Attack,	
Budget Management	
C	
Call Control	20-2
Call Filtering	16-1
Call Filters	
Built-In	16-1
User-Defined	16-1
Call Scheduling	23-1
Maximum Number of Schedule Sets	23-1
PPPoE	23-3
Precedence	23-1
Precedence Example	See Precedence
CDR	18-7
CDR (Call Detail Record)	18-6
CHAP	5-5
Collision	18-3
Command Interpreter Mode	20-1
Command Mode	18-9
Community	17-2
Connecting a POTS Splitter	2-4
Connecting the Prestige	2-3
Connections	
Additional Requirements	2-3
ADSL Line	2-3

Power Adapter	2-3	DHCP	1-4, 18-4
Rear Panel	2-2	DHCP Negotiation and Syslog Connection from the Internet – EG 3	13-4
Console Port	18-3	DHCP Negotiation	13-4
Content Filtering	15-1	Diagnostic.....	18-8
Days and Times	15-1	Diagnostic Tools.....	18-1
Keywords	15-1	Digital Subscriber Line Access Multiplexer.....	1-6
Log Records	15-1	DNS	4-10
Update List	15-1	Domain Name.....	8-17
Copyright.....	ii	Domain Name System.....	4-4
Cost Of Transmission	5-8, 6-6, 6-10	DoS	
Country Code.....	18-4	Basics	9-3
CPU Load	18-3	Types.....	9-4
Custom Ports		DoS (Denial of Service)	1-2
Creating/Editing	13-3	DSL (Digital Subscriber Line)	xxvii
Introduction	13-1	DSL, what is it?	xxvii
Customer Support	vi	DSLAM.....	See Digital Subscriber Line Access Multiplexer
Customized Services.....	13-2	Dynamic DNS	3-1
D		Dynamic Host Configuration Protocol	4-4
Data Filtering.....	16-1	DYNDNS Wildcard.....	3-2
DDNS		E	
Configuration.....	3-3	E-mail	
Default Policy Log.....	12-5	Log Example	11-5
Denial of Service	9-2, 9-3, 10-2, 11-7	Mail Server.....	11-4
Denial of Services		Mail Subject	11-4
Thresholds	11-9	Tab	11-3
Destination Address.....	12-3, 12-11	E-mail Alerts	11-4
Device Filter rules.....	16-16		

Encapsulation.....	1-5, 4-11, 4-16, 5-2	Filter Log.....	18-7, 18-8
ENET ENCAP	4-11	Filter Rule	16-10
PPP	4-12	Filter Rule Process.....	16-3
PPP over Ethernet	4-12	Filter Rule Setup	16-9
RFC 1483.....	4-12	Filter Rules Summary	
Error Log.....	18-5	Sample.....	16-19
Error/Information Messages		Filter Set	
Sample	18-6	Class	16-9
Ethernet Encapsulation	8-16	Filtering	16-1, 16-9
Ethernet Traffic	16-20	Filtering Process	
Example Internal SPTGEN Screens.....	L	Outgoing Packets.....	16-2
F		Firewall	
FCC.....	iii	Access Methods.....	10-1
Filename Conventions.....	19-1	Activating	10-2
Filter.....	3-5	Address Type.....	12-12
Applying Filters	16-19	Alerts	11-2
Ethernet traffic	16-20	Connection Direction.....	12-3
Ethernet Traffic.....	16-20	Creating/Editing Rules	12-9
Filter Rules	16-7	Custom Ports	See Custom Ports
Filter Structure	16-4	E-mail	11-2
Generic Filter Rule	16-14	Enabling	11-2
Remote Node	5-8	Firewall Vs Filters	9-12
Remote Node Filter.....	5-8	Guidelines For Enhancing Security	9-11
Remote Node Filters	16-20	Introduction	9-2
Sample	16-18	LAN to WAN Rules	12-3
SUA	16-16	Log	10-2
TCP/IP Filter Rule	16-9	Log Timer.....	11-4

Logs	11-3	Hop Count	5-8, 6-10
Policies	12-1	HTML Help	See
Remote Management.....	10-1	HTTP.....	8-17, 9-1, 9-3, 9-4, 25-11, 25-12
Rule Checklist	12-1	HyperTerminal program.....	19-6, 19-9
Rule Logic	12-1	I	
Rule Precedence	12-4	IANA.....	4-2, 4-3
Rule Security Ramifications.....	12-2	ICMP echo.....	9-6
Services	12-6	Idle Timeout	5-3
SMT Menus.....	10-1	IGMP support.....	5-8, 6-6
Types	9-1	Initialization.....	2-7
When To Use.....	9-13	Interactive Applications.....	22-1
Frame Relay.....	1-6	Internal SPTGEN	1-2, 28-1
Front Panel		FTP Download Example	28-3
Illustration	2-1	FTP Upload Example	28-4
FTP	19-4, 21-2, 21-3	Points to Remember	28-2
FTP File Transfer.....	19-10	Text File	28-1
FTP Restrictions	19-4, 21-3	Internal SPTGEN Screens	L
FTP Server.....	8-25	Internet access	4-1
Full Rate	2-4	Internet Access xxiv, 1-1, 1-6, 1-7, 2-12, 3-5, 4-1, 4-13, 4-15, 4-16	
G		Internet Access Setup	8-6
Gateway	6-9	Internet Assigned Numbers Authority..	See IANA
Gateway Node	7-3	Internet Control Message Protocol (ICMP).....	9-6
General Setup	3-1	IP Address . 4-10, 6-5, 6-9, 7-3, 16-11, 18-4, 18-9, 22-3	
H		IP Address Assignment	4-12
Half-Open Sessions	11-7	ENET ENCAP	4-12
Hidden Menus.....	2-11	PPPoA or PPPoE.....	4-12
hop count	6-6		

RFC 1483.....	4-12	ISDN.....	2-6
IP Alias Setup	4-6	K	
IP Filter	16-13	Key Fields For Configuring Rules.....	12-2
Logic Flow.....	16-12	L	
IP mask	16-11	LAN.....	18-3
IP network number.....	4-2	LAN to WAN Rules	12-3
IP Packet	16-14	LAND.....	9-4, 9-6
IP Policies	22-5	Link type.....	18-2
IP Policy Routing (IPPR).....	1-4, 4-5	LLC-based Multiplexing.....	6-2
Applying an IP Policy.....	22-5	Local Network	
Ethernet IP Policies.....	22-5	Rule Summary.....	12-4
Gateway.....	22-5	Log and Trace.....	18-5
IP Pool.....	4-4	Log Facility.....	18-7
IP Ports.....	25-11, 25-12	Log Screen.....	14-1
IP Protocol	22-4	Logging Option.....	16-11, 16-15
IP Routing Policy	22-4	Login.....	5-5
IP Routing Policy (IPPR).....	22-1	Logs	14-1
Benefits.....	22-1	M	
Cost Savings	22-1	MAC address	7-3
Criteria.....	22-1	Mail Server	11-4
Load Sharing.....	22-1	Main Menu	2-11
Setup	22-2	Management Information Base (MIB).....	17-2
IP Routing Policy Setup.....	22-3	Maximum Incomplete High.....	11-9
IP Spoofing	9-4, 9-7	Maximum Incomplete Low	11-9
IP Static Route	6-7	Max-incomplete High.....	11-7
IP Static Route Setup	6-8	Max-incomplete Low.....	11-7, 11-10
IPSec standard.....	1-2	MBS.....	See Maximum Burst Size

Media Access Control.....	7-1	O	
Message Logging.....	18-5	One Minute High.....	11-9
Metric.....	5-8, 6-6, 6-10	One Minute Low	11-9
Multicast	5-8, 6-6	One-Minute High	11-7
Multiplexing		P	
LLC-based.....	4-11	Packet	
VC-based.....	4-11	Error	18-2
Multiplexing	1-5, 4-11, 4-16, 5-2	Received.....	18-3
Multiprotocol Encapsulation.....	4-12	Transmitted	18-3
My WAN Address	5-7, 6-5	Packet Filtering.....	9-13
N		Packet Filtering Firewalls.....	9-1
Nailed-Up Connection	5-3	Packet Information	14-2
NAT	16-16	Packet Triggered.....	18-7
Application	8-3	Packets.....	18-2
Applying NAT in the SMT Menus.....	8-6	PAP.....	5-5
Configuring	8-8	Password.....	2-7, 2-13, 5-5, 17-2
Definitions	8-1	Ping.....	18-9
Examples	8-20	Ping of Death.....	9-4
How NAT Works	8-2	Point-to-Point	xxvii
Mapping Types.....	8-4	policy-based routing	22-1
Non NAT Friendly Application Programs	8-28, 8-29	POP3.....	9-3, 9-4
Ordering Rules	8-13	Port Configuration.....	13-4
What NAT does.....	8-2	POTS	2-4
NetBIOS commands	9-6	POTS Splitter	2-5
Network Address Translation (NAT)	8-1, 21-1	PPP	5-2
Network Management	1-5	PPPoA Encapsulation.....	6-2
		PPP Log.....	18-7, 18-8

PPPoE Encapsulation.....	5-3, 5-9	Restore Configuration.....	19-7
Precedence	22-1, 22-4	Return address	11-4
Prestige Firewall Application.....	9-3	RFC-1483	5-2
Prestige Web Configurator.....	11-1	RFC-2364	5-2, 5-4
Private	5-8, 6-6, 6-10	RIP	4-10, 5-8, 6-6. See Routing Information Protocol
Protocol.....	16-10	Routing Information Protocol.....	4-3
Protocol Filter rules.....	16-16	Direction.....	4-3
Q		Version	4-3
Quality of Service	22-1	Routing Policy	22-1
R		Rule Summary	12-4, 13-8, 15-1
RAS.....	18-4, 22-2	Rules	12-1, 12-4
Rate		Checklist.....	12-1
Receiving.....	18-2	Creating Custom.....	12-1
Transmission.....	18-2	Key Fields	12-2
Related Documentation.....	xxiv	LAN to WAN	12-3
Remote DHCP Server	4-10	Logic.....	12-1
Remote Management	21-2	Predefined Services	12-6
Firewall.....	10-1	Source and Destination Addresses	12-11
Remote Management and NAT	21-4	Summary	12-4
Remote Management Limitations	19-4, 21-3	Timeout	12-13
Remote Node	5-1, 18-2	S	
Remote Node Profile	5-4	SA Monitor	26-1
Remote Node Setup	5-1, 5-2	Sample IP Addresses	6-3
Remote Node Index Number	18-2	Saving the State	9-7
Remote Node Traffic	16-22	Schedule Sets	
Required fields.....	2-11	Duration.....	23-2
RESET Button	2-3	SCR.....	See Sustain Cell Rate

Security Association	26-1	Static Route Setup	6-6
Security In General	9-12	Static Routing Topology.....	6-7
Security Ramifications.....	12-2	SUA (Single User Account)	See NAT
Server.....	8-5, 8-9, 8-12, 8-15, 8-16, 8-17, 8-18, 8-22, 8-24, 20-5	Subnet Mask	4-2, 4-10, 5-7, 6-5, 6-9, 12-12, 18-4
Service	v, 12-2	Support Disk	xxiv
Service Type	13-3	Supporting Disk.....	xxiv
setup a schedule	23-2	SYN Flood.....	9-4, 9-5
Single User Account	4-17	SYN-ACK	9-5
SMT Menu Overview	2-10	Syntax Conventions.....	xxvi
SMTP Error Messages.....	11-5	Syslog	13-4, 18-6
Smurf	9-6	Syslog IP Address	18-7
SNMP		Syslog Server.....	18-6
Community.....	17-3	System	
Configuration.....	17-2	Command Interpreter Mode	18-9
Get	17-2	Console Port Speed	18-5
Manager.....	17-2	Diagnostic	18-8
MIBs.....	17-2	Log and Trace	18-5
Trap	17-2	Syslog and Accounting	18-6
Trusted Host	17-3	System Information.....	18-3
Source & Destination Addresses	12-11	System Status	18-1
Source Address	12-3, 12-10	System Information	18-3
Source-Based Routing	22-1	System Information & Diagnosis	18-1
Splitters.....	2-4	System Maintenance....	18-1, 18-3, 19-2, 19-5, 19-13, 19-14, 20-1, 20-2, 20-4
SPTGEN Screens.....	L	System Management Terminal	2-10
Stateful Inspection	1-2, 9-1, 9-2, 9-7, 9-8	System Parameter Table Generator	28-1
Prestige	9-9	System Status	18-2
Process.....	9-8	System Timeout.....	21-4

T		U	
TCP Maximum Incomplete.....	11-7, 11-8, 11-10	UDP/ICMP Security	9-10
TCP Security	9-10	UNIX Syslog	18-5, 18-7
TCP/IP	6-1, 9-3, 9-4, 16-16, 18-9, 21-1	UNIX syslog parameters.....	18-6
TCP/IP Options	6-1	Upload Firmware	19-10
TCP/IP Parameters	4-2	Upper Layer Protocols	9-10, 9-11
Teardrop.....	9-4	V	
Telephone Microfilters.....	2-5	VC-based Multiplexing	5-2, 6-1
Telnet	21-1	Virtual Private Network.....	1-1
Telnet Configuration	21-1	VPI & VCI.....	4-11
Telnet Under NAT	21-1	W	
Text File Format	28-1	WAN to LAN Rules	12-4
TFTP and FTP Over WAN}	19-4, 21-3	Web.....	21-2
TFTP File Transfer.....	19-12	Web Configurator	9-2, 9-11, 10-2, 11-1, 12-2
TFTP Restrictions	19-4, 21-3	Login	11-1
Three-Way Handshake.....	9-5	Password.....	11-1
Threshold Values	11-6	X	
Time and Date Setting.....	20-4, 20-5	XMODEM protocol.....	19-2
Time Zone.....	20-5	XMODEM upload	2-8
Timeout.....	12-13, 12-14	Z	
To avoid damage to the Prestige	2-3	ZyNOS.....	19-1, 19-2
TOS (Type of Service).....	22-1	ZyNOS F/W Version	19-1
Trace Records	18-5	ZyXEL Limited Warranty	
Traceroute	9-7	Note	v
Transfer Rate.....	18-3	ZyXEL's Firewall	
Transmission Rates	xxiv, 1-1	Introduction	9-2
Type of Service	22-1, 22-3, 22-4, 22-5		

